HOUSE OF LORDS

Science and Technology Committee

5th Report of Session 2006–07

Personal Internet Security

Volume II: Evidence

Ordered to be printed 24 July 2007 and published 10 August 2007

Published by the Authority of the House of Lords

London : The Stationery Office Limited
£price

HL Paper 165–II

CONTENTS

Oral Evidence

Written Evidence

Note: The Report of the Committee is published in Volume I (HL Paper 165-I).

Minutes of Evidence

TAKEN BEFORE THE SELECT COMMITTEE ON SCIENCE AND TECHNOLOGY (SUB-COMMITTEE II)

WEDNESDAY 29 NOVEMBER 2006

Present	Broers, L (Chairman)	Sharp of Guildford, B
	Howie of Troon, L	Sutherland of Houndwood, L
	O'Neill of Clackmannan, L	Young of Graffham, L
	Patel, L	

Memorandum by the Government (Home Office and the Department of Trade and Industry)

Security issues affecting private individuals when using communicating computer-based devices, either connecting directly to the Internet or employing other forms of inter-connectivity

SUMMARY

The Introduction sets out our approach to the written evidence and highlights some of the key issues around security issues affecting private individuals when using the Internet.

In Section 1, we define what we know about the problem of security threats to private individuals by discussing the emergence of virtual organised crime groups who are organised and operate exclusively via the Internet. We highlight some of the methods used by the groups to exploit the Internet and give some statistics to demonstrate the scale of the problem. We end this section by discussing research which suggests that users do not understand the nature of online threats.

In Section 2, we discuss how we are currently tackling the problem of security issues affecting private individuals. We highlight the potential concerns/trade-offs. We detail some of the positive work being done via public and private initiatives, such as Get Safe Online (GSOL), to raise awareness of the risks online. GSOL brings together government, industry and law enforcement to give people advice, guidance and the tools they need to be safe online. We highlight the importance of national and international co-operation to the threats and the Serious Organised Crime Agency (SOCA)'s role in ensuring this. We discuss how software and hardware can play a fundamental role in reducing the risk of security breaches, but caveat this by pointing out that technical solutions alone will not work. We end this section by highlighting a new initiative to improve the standing of UK research in this area.

In Section 3, we look at the issue of IT governance and regulation. In terms of IT governance, we discuss initiatives that both industry and government are undertaking that appear to be impacting on the security threat. We discuss how security breaches that take place in this country can be instigated in another jurisdiction and the global nature of this issue. We therefore draw attention to some of the work being done internationally to ensure international law enforcement co-operation. When looking at regulations we discuss the fact that the regulatory framework is a mixture of international, EU, UK and industry regulations, which means that at times enforcing these can be challenging.

We stress that over-regulation could affect our ability to create and maintain a flexible framework that keeps abreast of industry changes and could impact on the ability to provide innovative services and products.

We end this section by discussing how cost and funding, timely assessments, technical ability and end use of systems are the main barriers to developing security systems and standards. We briefly discuss how these problems can be overcome.

In Section 4, we look at crime prevention. We highlight the various activities through which the Government delivers crime prevention and discuss some of the current changes to legislation which will ensure that UK criminal law continues to meet the challenge of e-crime. We end this section by giving a flavour of the international actions on e-crime.

Introduction

The Government is working collaboratively to protect private individuals from Internet security threats. Reflecting this joined up approach, this evidence is submitted by Home Office and DTI Ministers and encompasses work being undertaken by the key Departments and Agencies. These are:

- Home Office—responsible for public protection, including in this context policy on criminal law and policing;
- the Department of Trade and Industry (DTI) responsible for promoting the business and consumer benefits of the information age and the regulatory framework for service providers;
- the Serious Organised Crime Agency (SOCA), an intelligence-led agency with law enforcement powers, created to reduce the harm caused by organised crime to the UK; and
- the Cabinet Office responsible for the co-ordination of security policy overall and the delivery of the Government's information assurance strategy.

Together, the efforts of these Departments and Agencies should help to create a culture of security online which maximises the benefits of using the internet, minimises the risks and tackles organised crime's exploitation of it.

This submission also recognises that changing the way in which individuals think about and use the Internet is a challenge, and Government, users and industry, all have a role to play. We therefore discuss the ways in which we work to ensure we deliver the right combination of informed users, appropriate regulation and relevant technology to promote a culture of security. We appreciate that without all three there is a danger that individuals will not understand and address the risks and that industry will put innovation above safety.

This submission also seeks to demonstrate how we actively support awareness raising through joint industry/government projects such as the Get Safe On Line initiative.

This submission deals only with security issues in the sense of users' control of their technology or their personal information being compromised, rather than wider internet safety issues such as child protection or content regulation where there are many developments and a strong track record of Government and industry working together to develop self-regulatory solutions to issues like illegal images of child abuse. For consistency, we describe this as "e-crime".

Section 1: Defining the Problem

1. *What is the nature of the security threat to private individuals? What new threats and trends are emerging and how are they identified?*

The last 3–4 years has seen the emergence of virtual organised crime groups (OCGs) who are organised and operate exclusively via the Internet. Their membership is geographically dispersed and multinational. Their main goal is the exploitation of the Internet to steal personal data and identity information (commonly called "identity theft") to facilitate fraud. These groups are growing in size, number and sophistication.

The UK has attracted the attention of these organised crime groups because of its relative affluence and speed of adoption of the Internet by individuals to buy goods and services online. There are 17 million Internet bank accounts in the UK and over £20 billion was spent online last year by UK customers. Attacking English-speaking countries may also pose fewer linguistic challenges than similar attacks on, for example, Japan.

These groups seek to compromise the integrity of personal data using a variety of methods, targeting both individuals and enterprises which hold customer records. Attacks against individuals can be considered in two main categories: malicious software and "social engineering". Malicious software attacks are used to compromise home and small business machines. Once infected the malicious code is used to "harvest" personal data while the user is online. "Social engineering" refers to attacks, typically aimed at home users, which are intended to trick individuals into revealing sensitive personal information, such as bank login data and credit card details.

In the past, attacks have tended to be large-scale and as a result attracted a higher profile. This tended to limit their effectiveness, because users were more likely to become aware of the threat and update their anti-virus software, and because their high rate of incidence made them more readily detectable by anti-virus companies. Attack patterns appear to be changing—malicious software is now typically distributed on a smaller scale, making it harder to detect. The software has become more sophisticated, and is often designed to disable or evade anti-virus systems, work in a phased approach to open back doors to systems and, increasingly, embed itself in the operating system to avoid detection. Some aspects of online behaviour are inherently more risky than others: "unofficial" file sharing sites offering music or video files are often used to mount malicious software attacks. Pirated software applications are inherently riskier than licensed versions and obviously more difficult to keep their security features up to date.

Criminals are also targeting corporate networks to steal information, usually financial data, held on customer databases. Targets include e-Commerce sites, credit reference agencies and third party card processing agencies. Successful hacking attacks on these types of firm can yield huge amounts of personal information that can then be exploited by fraudsters. Globally, the worst reported incident is last year's hack of CardSystems Inc, a US credit/debit card processing company which resulted in the compromise of 40 million credit card accounts, with fraud confirmed on a minimum of 250,000 accounts.

Although fraudulent transactions can be readily identified by banks and other financial institutions, it is difficult to assess what percentage of fraudulent activity is directly attributable to Internet attacks, as the exploitation of the Internet is one of several avenues used to obtain personal information. However, the financial services industry has made significant progress in identifying Internet attacks while they are underway, making effective mitigating action a realistic prospect in more situations than previously.

2. *What is the scale of the problem?*

There are many varying statistics referring to the scale of the problem. For example:

- one in every 52 emails in January and one in 28 emails in June 2005 were affected with malicious content (IBM);
- in 2004, total losses from online banking fraud were recorded for the first time and reached £12.2 million (APACS 2005). In 2005, online banking fraud grew to £23.3 million, an increase of 90 per cent from 2004;
- when asked which of a series of crimes individuals felt most at risk of in their everyday lives, 21 per cent identified Internet crime (higher than burglary 16 per cent, mugging 11 per cent or car theft 8 per cent) (GSOL survey Oct 2006);[1]
- the 2003–04 British Crime Survey found that 27 per cent of adults who used the Internet at home reported their computer had been affected by a virus (a third of those reported the computer had been damaged) in the previous 12 months. Two per cent of adults who used the Internet at home reported their computer had been accessed or files hacked into on their home computer in the previous 12 months.[2]

These statistics must be set against the increasing level of transactional usage of the Internet by the general public and small businesses:

- the UK is now one of the leading e-commerce economies in the world. The volume of online card payments has increased five-fold over the last five years, reaching 310 million for a total of £22 billion. This accounts for five per cent of all personal card payments. There are over 17 million Internet bank accounts in the UK; and
- more than 50 per cent of small businesses conduct transactions over the Internet on a regular basis (APACs September 05).

It should be noted that we are also seeing a significant shift in the Internet being used socially. A recent statistic from the IMRG (Interactive Media in Retail Group) indicates that the average web user spends more time online than watching television. Broadband "chat" now competes with daytime TV for the attention of women. This all means that people are spending more and more of their daily lives on the Internet.

[1] www.getsafeonline.org/media/GSO_Cyber_Report_2006.pdf
[2] www.homeoffice.gov.uk/rds/pdfs06/rdsolr0906.pdf

3. *How are security breachers affecting the individual user detected and recorded?*

Not all personal users will be immediately aware that there has been a security breach. Increasingly, breaches are designed to run clandestinely on the machine and to evade firewall and anti-virus detection. On machines that do not have up to date protection, breaches are even less likely to come to light.

Even where the user identifies they have been the victim of a breach, there is a great variation in response. According to the British Crime Survey, fewer than four in 10 of those who knew their computers were infected by a virus reported the incident at all. Of them, nine per cent reported to an ISP, 13 per cent to a website administrator and one per cent to the police.

A number of private sector companies regularly comment on the changing nature and the extent of internet problems and industry bodies such as the the US-based SysAdmin, Audit, Network, Security (SANS) Institute do annual reviews of the key vulnerabilities. The DTI's biennial surveys measure the impact of information security breaches on UK business—not just those that arise from connection to the Internet—and the measures that are being taken to prevent damage.

4. *How well do users understand the nature of the threat?*

This is almost impossible to quantify, but see paragraph 6 for known information relating to the level of public awareness.

However, the Office of Fair Trading has commissioned a wide-ranging market study into Internet Shopping[3] due to be published in spring 2007. The market study is exploring, through consumer research and stakeholder consultation, the scale of any mismatch between consumer fears and actual risks, as well as how these fears might be addressed.

Section 2: Tackling the Problem

5. *What can and should be done to provide greater computer security to private individuals? What, if any, are the potential concerns and trade-offs?*

Both Government and industry have roles in ensuring that people are aware of the general risks online. Both also have a critical role to play in ensuring that the public are conducting online transactions with them safely. The nature of the Internet means that it is our collective responsibility to ensure that people are doing what they can to make themselves and their families safe online so that they can enjoy the real benefits of the Internet.

Information, understanding and appropriate training are among the primary challenges in tackling the growing risk of Internet security threats, e-crime and online fraud. Simple, clear advice from one source is required to effectively improve the public's understanding of these threats and to encourage people to protect their personal information and electronic devices when online. Get Safe Online brings together Government, industry and law enforcement in a partnership to resource a campaign to give people the advice, guidance and the tools they need to be safe online (see next section).

Increasingly computer retailers and manufacturers are providing additional security and safety software as part of a home computer package. Furthermore, many application software providers are incorporating more security features in their programs and organisations heavily reliant on online money transactions have for sometime offered free security products. However, although products are widely available and strongly marketed, there is reluctance amongst users to install and use them. The main reasons seem to be that installing packages is perceived by users: to be complex and cumbersome; to restrict choice by filtering sites/emails; to require regular time consuming security screening; costly (most work on the basis of monthly/annual subscription to receive regular updates). Even the take up of free programs offered via reputable organisations such as banks has been disappointingly low with only about five per cent of online customers using this service.

We actively encourage users to assess risks and to put in place measures to mitigate those risks. For most users, off the shelf products provide the appropriate level of protection, however, in some circumstances such as banking online or registering tax returns more is required. In these cases, identity is the key issue and two factor authentication is becoming the preferred method of identifying the person or organisation you are interacting with. The Government is looking seriously at the whole issue of managing identity

[3] http://www.oft.gov.uk/news/press+releases/2006/81-06.htm

online. It is a key feature of Sir David Varney's work on transforming Government and the Chancellor of the Exchequer has asked Sir James Crosby to lead a piece of work on identity and the respective interests of the private and public sectors.

The ISPs have a particular role in relation to the security of their customers and many offer security scanning and spam filtering services. We are in discussion with the ISPs as to how the industry might continue to make forward momentum in this area and demonstrate leadership in dealing with these problems.

6. *What is the level of public awareness of the threat to computer security and how effective are current initiatives in changing attitudes and raising that awareness?*

There are a range of public and private sector initiatives underway to raise public awareness of e-crime and the basic steps users can take to protect themselves. These include Get Safe On Line (GSOL), Bank Safe On Line, IT Safe and Fraud Alert. Between them they represent an important step forward in reducing the public's exposure to the risks of online fraud and data theft.

The Get Safe Online[4] campaign launched in 2005 aims to raise awareness of the risks people face online and provide them with independent, authoritative advice, guidance and tools to help keep themselves and their families safe on the Internet. The campaign brings together several government departments and agencies (including the Cabinet Office, Home Office, DTI and SOCA) and involves some well-known UK and international private sector brand names including BT, Dell, eBay, HSBC, Lloyds TSB, MessageLabs, Microsoft, securetrading and Yell.com. Importantly, Get Safe Online has from the outset sought to measure public awareness to ensure that its messages are having an impact.

The Get Safe Online website now has over 13,000 links to it. The 2005 campaign included road shows in 12 cities across the UK. Research was carried out before and after the campaign. The results showed that there was a very good level of awareness of the campaign and some indications of a shift in behaviour:

- three per cent of respondents were aware of the campaign or logo within one month of the launch of the campaign, and of these:
  - 62 per cent recognised the need to be careful when being online;
  - 52 per cent recognised it was their responsibility to stay safe;
  - 52 per cent understood the potential risks;
  - 40 per cent said that they had been prompted to find out more;
- awareness of threats such as key-logging and phishing[5] rose by 15 per cent and 12 per cent respectively;
- behaviour change had the greatest impact on backing-up data (75 per cent of those aware of the campaign did compared with 53 per cent of the non-aware).

After the campaign, respondents were:

- more likely to have installed a firewall or anti-spy software;
- Significantly more likely to back up their data;
- significantly more likely to keep personal details private;
- more likely to use and update anti-virus and anti-spyware tools regularly.

19 per cent of respondents felt less secure once aware of the risks whilst 24 per cent felt more secure through increased knowledge and reassurance that they were doing the right thing.

A second phase of Get Safe Online activity was launched on 9 October 2006 and achieved a good level of national and local media coverage. Road shows were run in eight cities across the UK in shopping centres, libraries, community centres and town halls and providing training at UK Online centres.

[4] www.getsafeonline.org

[5] Phishing a type of fraud that tricks users into visiting malicious websites, typically through "spoofed" emails from well known banks, online retailers and credit card companies. Ofcom Online Protection Report June 2006.

The main findings of the Get Safe Online Report October 2006[6] are:

- Fear of e-crime is increasing. When asked whether they felt more at risk from bank card fraud, burglary, car theft and mugging, 21 per cent of people thought that Internet crime is the crime they are most likely to encounter. This is compared to 17 per cent who were most afraid of Internet crime a year ago.
- 24 per cent of people have been deterred from Internet banking, more than a fifth (21 per cent) will not do their financial management online, 18 per cent will not shop online and one in six (17 per cent) have been put off using the Internet all together, as a result of concerns about e-crime.
- Three quarters of respondents look to people/organisations other than themselves to take responsibility for Internet safety. Over 40 per cent felt it should be the responsibility of the big online organisations to insure them against online fraud.
- Knowledge gap—72 per cent said they needed further information about online safety and 40 per cent were still not sure where to go for advice.
- A significant proportion of those surveyed (35 per cent) still go to friends and family first for advice about online safety, but encouragingly, a quarter are turning to websites like GSOL.

The report indicates that there has been a shift in people accepting that it is primarily their own responsibility to make sure they are safe when online. A quarter thought it was their responsibility to make sure they are safe online, compared to only 15 per cent last year, but 41 per cent felt it was the job of big online organisations to protect them from online fraud.

7. *What factors may prevent private individuals from following appropriate security practices?*

Security is perceived as, at best, time-consuming and dull and, at worst, expensive and someone else's problem. Many people feel that it is too time-consuming to do anything about their Internet security and many of the technical terms used discourage users from investing their time.

Get Safe Online aims to instil a sense of personal responsibility into PC users as well as offering advice and help to ensure they protect their personal details online. The campaign encourages people to use the same kind of common sense on the Internet that they would apply when out on the high street: "You wouldn't do this (ie give out your personal details) on the street—so why do it on the web?" was the strapline for the campaign.

Another reason why PC users may be discouraged from taking adequate security measures is the cost of security products (Internet access can be relatively cheap whilst a firewall and anti-virus package can cost about £50).

There is a move away from Internet connection via fixed computers with users increasingly accessing the Internet through mobile phones, games consoles and other devices. This leads to a new challenge in both making the technology secure and raising awareness of reasonable precautions that may be taken by users.

8. *What role do software and hardware design play in reducing the risk posed by security breaches? How much attention is paid to security in the design of new computer-based products?*

Hardware and software design is fundamental in reducing the risk posed by security breaches, and can also play a major role in highlighting the potential for, and the incidence and impact of, such breaches.

It is probably fair to say that until recently security was not a key factor in designing many software or hardware products. In fast-moving industries like these, there is an inherent tension between getting a product to market and making sure it is a failsafe product. This problem becomes more challenging as products become even more complex and used in more situations.

Bill Gates' memo to all Microsoft staff in 2001 indicating that the company had to turn round its performance on security was a turning point in this regard. There has been a shift towards software designers adopting engineering principles to review and identify vulnerable codes, which has resulted in employees being trained in developing more secure code to avoid future vulnerabilities.

[6] www.getsafeonline.org/media/GSO_Cyber_Report_2006.pdf

Although more secure coding will reduce software vulnerabilities is to be welcome, the increasing complexity of software will perhaps continue to give rise to new vulnerabilities There is also usually a time lag between the vulnerability being discovered and the software producer developing a "patch" that resolves the problem. During this time users are exposed to hackers exploiting the vulnerability.

Another important development, in relation to hardware, is the collaborative effort of the ICT vendors to produce a Trusted Computing kernel to be incorporated in the next generation of PCs. This will enable applications to more easily utilise the inherent functionality of the PC to deploy security solutions.

Again, it is important to note that technical solutions on their own do not work. Awareness raising, regulation and appropriate enforcement are vital in developing a secure Internet. Applications and hardware are tools with which to combat and reduce security threats, not a means of eradicating them.

9. *What is the standing of UK research in this area?*

We understand that the UK Research Councils will respond separately to this consultation. They will have a view on the standing of UK research. However we thought it useful to give a brief over view of a relatively new initiative, Innovation Platforms and Knowledge Transfer Networks (KTN),[7] aimed at strengthening the UK standing in this important area of research.

Innovation platforms have been developed by the DTI Technology Strategy Board[8] to respond to a well defined societal challenge where Government Departments/Agencies, Research Councils, RDAs/DAs, business and the science base can work together. The first step towards an innovation platform in network security has been the establishment of a core group of partners. This core group provides policy oversight and has helped to develop a business and research community around network security.

Future activities are expected from the DTI led Technology Programme. These will run alongside activities from other Government Departments, Research Councils and the DTI's own Cyber Security KTN to bring forward successful and co-ordinated innovative solutions in the area of online security.

The area of Human Machine Interface[9] has been included in the list of technology priorities recently released for the Autumn 2006 and Spring 2007 competitions for Collaborative Research and Development (CR&D) projects in the Technology Programme. In order to strengthen network security there is a need to address human, as well as technological, vulnerabilities. The competition in Human Machine Interface in Network Security will be looking to support projects that address the challenge of effective communication of security to the non-specialist user and new systems and environmental design to reduce insider fraud. This is a "challenge-driven" approach, encouraging consortia to focus on achieving solutions to a societal challenge. Support will be in two stages—initially through supporting short feasibility studies, the best of which will be selected, leading to longer-term collaborative research and development projects, with the ability to make significant change.

The Technology Strategy Board, Innovation Platforms and KTNs output and activity are aimed at stimulating innovation in areas such as security and informing government thinking.

Foresight, another DTI research initiative has also carried out independent work in this area, see its 2004 project on Cyber Trust and Crime Prevention.[10]

Section 3: Governance and Regulation

10. *How effective are initiatives on IT governance in reducing security threats?*

IT governance incorporates international, national and UK regulation as well as self-regulation. The online threat landscape[11] is complex with wave upon wave of threats to the user. Responding to the ever-changing threat from diverse sources and locations means the regulatory framework requires flexibility. As a consequence, the UK regulatory framework consists of self-regulation underpinned by supporting legislation.

[7] http://www.ktnetworks.co.uk/epicentric_portal/site/cys/

[8] http://www.dti.gov.uk/innovation/tech-priorities-uk/tsb/index.html

[9] The human-machine interface (HMI) is where people and technology meet. This people-technology intercept can be as simple as the grip on a hand tool or as complex as the flight deck of a jumbo jet (definition used by International Engineering Consortium).

[10] http://www.foresight.gov.uk/previous_projects/cyber_trust_and_crime_prevention/index.html

[11] For example, many home users have antivirus software and firewalls, which limit the chances of malware being downloaded accidentally, so increasingly phishing attacks are taking the form of directing users to websites via embedded hyperlinks.

There are a number of industry initiatives impacting on the threat landscape. Most ISPs provide some form of email filtering to their consumers to reduce the impact of spam. Some larger ISPs offer security advice either online or via an advice line, some provide their consumers with security products free of charge or at reduced cost, others offer a range of links to security sites so that customers can purchase reputable products, most have contractual clauses that terminate the service on the grounds of unacceptable behaviour (commonly referred to as Acceptable Use Policy) and others are actively promoting public debate and awareness on security issues. Software providers are also involved in providing information, with some larger providers undertaking citizen programmes to raise security issues in schools and other public forums, circulating newsletters and security checklists.

The DTI has long promoted information security as a key business enabler and stressed the importance of a risk management approach[12]—that is one that applies appropriate resources to real problems in a timely manner. To this end, the Government has worked with the British Standards Institute to develop and promote three standards on information security management. The two key standards are now international standards and are starting to make an impact globally. One is a guideline on information security management (ISO 17799) and the other is a management system standard which allows for third party assessment of compliance (ISO 27001). These standards will enable, in effect, tools for companies to address information risk as part of their corporate governance objective to manage risk and will, in many cases, lead to decisions being taken that will add to the security of customers of these companies.

This year has seen the launch of the Institute of Information Security Professionals[13]—a development actively supported by DTI and the Cabinet Office. The Institute acts as an accreditation authority for the industry and it is anticipated that Membership and Fellowship of the Institute will be the internationally accepted gold standard "qualification" for information security professionals. By being able to recognise quality professionals working in the industry, individuals and companies will be more secure about the advice, services and products they provide or develop.

11. *How far do improvements in governance and regulation depend on international co-operation?*

The global nature and the pace of evolution of services put existing regulatory models and structures under real pressure to respond. Maintaining and improving governance and regulation can only be achieved through close working co-operation within the international community. In Europe, we have welcomed the creation of the European Network and Information Security Agency as a centre of expertise available for policy makers throughout Europe. It seeks to identify and spread best practice and has focused on the need for awareness raising at all levels of society. The World Summit on the Information Society is, through its work on Internet Governance, giving a global profile to the work to combat e-crime and deliver resilient services to users.

The UK Government works closely with other governments and agencies in mitigating as many online risks as possible. Already we have a memorandum of understanding (MoU) with countries such as the USA and Australia. We are constantly looking at ways of improving co-operation by increasing the number of MoUs in operation or by developing more tailored ways of working together to improve security. We actively participate in Organisation for Economic Co-operation and Development (OECD) initiatives in this area.

From a consumer perspective, the Office of Fair Trading has developed good working relations with enforcers in other countries. Whilst the basis of this work is generally informal, the UK also participates in the International Consumer Protection and Enforcement Network (ICPEN) and the London Action Plan of anti-spam authorities, which spans 5 continents. Greater co-ordination between enforcers at both a national and international level is likely to lead to greater compliance and more effective enforcement.

12. *Is the regulatory framework for Internet services adequate?*

The regulatory framework is a mixture of international, EU and UK regulation and industry self-regulation. Whilst traditional regulation is difficult, the industry has a history of self-regulation in a number of areas. The recent Ofcom report "Online Protection: A survey of consumer, industry and regulatory mechanisms and systems",[14] provides evidence for this approach and suggests that where the industry self-regulates or co-regulates with an ombudsman of the Government there is a higher level of consumer protection.

[12] Risk management is simply a practice of systematically selecting cost effective approaches for minimising the effect of threat realisation to the organisation. Dorfman, Mark S (1997). Introduction to Risk Management and Insurance (6th ed) Prentice Hall.

[13] http://www.instisp.org/

[14] www.ofcom.org.uk/research/technology/onlineprotection/ Page 4, paragraph 1.7.

However, there is a more general issue in developing regulatory frameworks for environments such as the Internet. Over-regulation and the lack of ability to foresee technological change may affect our ability to create a flexible framework that keeps abreast of industry changes. Over-regulation may also stifle the Internet's unique ability to provide innovative services and products to meet user needs/demands or drive business offshore. The Government and other stakeholders are contributing to the debate around the revision of the overarching framework applying the regulation of electronic communications. The Commission have indicated that the security of networks and the problems impacting directly on consumers will need to be addressed in this process.

The remit of the Office of Fair Trading's fact-finding market study is limited to consumer protection rather than general security issues. Within this remit, early evidence suggests that the regulations are generally considered by a range of stakeholders (businesses, trade bodies, consumer groups and public sector organisations) to be broadly "fit for purpose". However, the picture appears more complicated when looking in detail at the four "case study" sectors (music, airline tickets, electrical and online auctions), each of which raises specific regulatory issues.

13. *What, if any, are the barriers to developing information security systems and standards and how can they be overcome?*

The DTI industry survey has shown that the level of investment in information security is rising but that there is still a significant skills gap and lack of awareness of the changing nature of the problem. It is by no means clear that there are significant barriers to the development of security standards—indeed there is an enormous amount of activity—but rather that the standards are not being applied in an effective manner. This relates to the skills gap identified in the DTI survey.

At both national and international levels, a number of security standards are being developed. Within Europe (ETSI, CEN, CENELEC) this process is voluntary, and supported by organisations. Only limited funds are made available by the European Commission or national Governments and as such it is very much driven by those who have an interest and the time to undertake the work. The same holds for worldwide standards (where IETF, W3C, ITU are prominent).

Standard setting requires expertise in technical areas. There is a limited supply of technical experts and they are spread thinly. The recently launched Institute of Information Security Professionals will help in raising the standing of the profession and should attract more engineers to specialise in it in the medium-term. The low levels of engineering postgraduates is an ongoing issue that has been taxing UK educationalists for a number of years and there are no easy solutions to this problem.

Schemes such as the Common Criteria and Claims Tested Mark provide some level of standardisation, however both schemes have problems. The Common Criteria takes time to test a product and is relatively costly. The Claims Tested Mark costs less and the process takes only weeks to complete but it only tests the claims of the manufacturer or provider of the service. In both cases, the mark awarded lasts for a number of years during which time products are updated and claims become outdated. The results are therefore a snapshot of the security at a given time and, more importantly, in isolation. Product assurance is a positive move in improving online security, however it is only effective if used appropriately.

Section 4: Crime Prevention

14. *How effective is Government crime prevention policy in this area? Are enforcement agencies adequately equipped to tackle these threats?*

Much of the Government's crime prevention activity in this area is delivered through Get Safe Online, as detailed above. However, there are a number of other activities, including:

— the ITSafe website[15] funded by the Home Office and the Cabinet Office provides home users and small businesses with alerts and advice drawn from NISCC[16] and a number of other sources on protecting computers, mobile phones and other devices from malicious attack;

[15] www.itsafe.gov.uk
[16] www.niscc.gov.uk

— a number of local police forces provide advice on their websites;[17]

— the DTI provides advice to small businesses through its website[18] and through business link service.[19]

Responding to the majority of crime relating to breaches of personal Internet security falls to local police forces. The total funding available to forces continues to rise and decisions on how to allocate those resources rest with Chief Constables. Since 2002, every police force in England and Wales has had its own computer crime unit of properly trained and equipped staff. These units have grown significantly in size over that period and the Home Office issued good practice guidance for managing them in 2004.

In addition, the Serious Organised Crime Agency (SOCA) has e-crime and fraud (including online fraud) among its priorities. SOCA is an intelligence-led agency with law enforcement powers, created to reduce the harm caused by organised crime to the UK. It was formed in April from a number of agencies, including the National Crime Squad and within that the National High Tech Crime Unit. SOCA has an e-crime directorate responsible for minimising the harm to the UK caused by e-crime and criminals' use of technology.

National and international co-operation is also a key element of the response to the threats. Police forces, HM Revenue and Customs and other agencies have interests in this area, and the various law enforcement interests are brought together in the National e-crime Strategy Group. SOCA is building on its inherited activities to develop a range of bilateral and multilateral partnerships with domestic and overseas law enforcement agencies to extend the reach of UK law enforcement's response to e-crime.

15. *Is the legislative framework in UK criminal law adequate to meet the challenge of cyber-crime?*

The Government is committed to ensuring that actions should be legal or illegal according to their merits, rather than the medium used, ie what is illegal offline should be illegal online and vice versa. As such, all legislation criminalises offences regardless of the means used to commit the offence.

Where there is a need to revise legislation to take account of new criminal techniques we seek to do so. We liaise regularly with the prosecution and law enforcement authorities to ensure the criminal law remains fit for purpose, but are not aware of significant legislative gaps that hinder the agencies.

For example, although the law relating to e-crime is generally fit for purpose, we have recently put before Parliament changes to the Computer Misuse Act 1990 to strengthen it. The changes will:

— Broaden the definition of the section 3 offence to clarify that that all means of interference with a computer system are criminalised—in particular ensuring that adequate provision is made to criminalise all forms of denial of service (DoS) attacks.

— Increase the maximum penalty for the section 1 offence of unauthorised access to computer material to two years to better reflect the seriousness of these offences as more and more sensitive systems and information have external connections and also ensure that the offence is extraditable. We are similarly proposing to increase the maximum penalty for the section 3 offence of unauthorised modification of computer material to 10 years.

— Create a new offence of making, adapting or supplying articles for use in computer misuse offences to discourage the market in the production and distribution of hacking tools (devices which can be utilised in the subsequent commission of offences of illegal access and systems and data interference). The new offence will allow us to will give effect to Article 6 of the Cybercrime Convention.

Another example is the Fraud Bill. It will create a general offence of fraud (rather than focusing on specific acts as previous fraud statutes have done and deals with them in a technology neutral way), with three different ways of committing it—a person will be guilty of the general offence if he is dishonest and either:

1. makes a false representation (including a false representation to a machine); or
2. fails to disclose information; or
3. abuses a position of trust.

[17] eg: www.met.police.uk/crimeprevention/computer, www.sussex.police.uk/comp_crime/comp_crime

[18] www.dti.gov.uk/sectors/infosec/

[19] www.businesslink.gov.uk

This will cover the full variety of fraudulent behaviour and should ensure that the offence continues to be relevant as methods of crime and technology change and develop. The bill also brings forward other new offences which will assist in combating e-crime—these include:

1. an offence of obtaining services dishonestly—this will plug a legal loophole whereby, for example, fraudsters obtain services over the Internet, but are not subject to the current law of fraud as they have not deceived a person;
2. various offences of possessing, manufacturing or supplying equipment, such as a computer programme that can generate genuine credit card numbers, to be used to commit or facilitate fraud.

16. *How effectively does the UK participate in international actions on cyber-crime?*

The UK is an active international player in relation to e-crime, both operationally and strategically.

UK law enforcement has strong links with operational colleagues overseas bilaterally, as well as through Europol, Interpol and the G8 contact network. International activity has tended to be focused through the National High Tech Crime Unit (now SOCA e-crime) and the Metropolitan Police Service and there are regular examples of successful investigations where UK law enforcement has been assisted by overseas colleagues or *vice versa*.

At the political level, the UK is actively involved in setting the agenda on e-crime in various fora within Europe, the G8 and the Commonwealth and elsewhere. For example, the UK has been a driving in helping develop a common global approach to e-crime legislation through the Council of Europe Cybercrime Convention and placed e-crime high on its JHA agenda during last year's presidencies of the EU and the G8.

Examination of Witnesses

Witnesses: Mr David Hendon CBE, Director of Business Relations 2 Management Unit, Mr Geoff Smith, Head of e-Business and e-Security, Business Relations 2 Management Unit, DTI, Mr Tim Wright, Head of Computer Crime, and Mr Stephen Webb, Head of Organised and Financial Crime Unit, Home Office, examined.

Q1 ***Chairman:*** Let me welcome everybody to this meeting of the House of Lords Select Committee for Science and Technology. This is our first session where we are taking evidence on the inquiry into Internet security which we have just begun. So let me welcome all of our witnesses and all the members of the public who have come today. There is a note which you can pick up if you have not already done so which gives the background to the inquiry and the Members of the Committee. Thank you very much for coming to talk to us, witnesses, and if we could start by you introducing yourselves and then we will proceed. Perhaps we could start with you, Mr Hendon.

Mr Hendon: Thank you. My name is David Hendon. I am Director of Business Relations 2 in the DTI. That title will not tell you very much about what I do, which is unfortunate, but I look after about half of the business sectors, the things which the DTI does for those sectors, and that includes all of the communications, IT, electronic sectors and the subject of this inquiry.

Mr Smith: I am Geoff Smith. I am Deputy Director of Information, Security and Internet Policy, which is part of David Hendon's command in DTI.

Mr Webb: I am Stephen Webb, Head of the Organised Financial Crime Unit in the Home Office. We have responsibility for a range of organised crime areas, the responsible unit for the Serious Organised Crime Agency and responsibility for e-crime.

Mr Wright: I am Tim Wright from the Home Office Computer Crime Team, which is part of the Organised Financial Crime Unit.

Q2 ***Chairman:*** Thank you very much. Would any of you like to make an opening statement? Then we will go straight into questions. I will ask the first question. What is your view of the adequacy of data on e-crime?

Mr Wright: We look at three sources in assessing the level of electronic crime; victim surveys, police recorded crime figures and then other sources, intelligence, insurance and other kinds of data. In relation to victim surveys for large and medium sized businesses we have a biennial DTI survey of security breaches. For households, the British Crime Survey has a specific module on technology crimes and there is a number of other reputable surveys around SMEs and around children's use of the Internet. In terms of victim surveys, we have put in place a reasonable set of victim surveys. The second source is police recorded crime. Most e-crime is a form of traditional crime like fraud, theft or

extortion, and therefore the police do not count e-crime separately to other forms of crime. We did some research on this in the Home Office and found that only a small number of forces were able to distinguish between e-crime and other forms of crime, and this is something we are working on with ACPO and HMIC for the future. Particularly in relation to e-crime there are many other sources of data from Honeynets, the IT security industry, ISPs, various sources of data, which we are not really making the best use of. This is something we are working with SOCA on for future years' threat assessments, to routinely gather that kind of information to give us a much clearer picture of the level of e-crime. I think we have good victim surveys. Police recording of e-crime is not what it ought to be and we have a clear solution in place for gathering other data and putting it all together.

Q3 ***Chairman:*** There is anecdotal evidence that there is rather a low level of incident reporting, particularly by individuals. What is being done to improve the level of reporting and how and by whom, and to what effect is the reported data processed?
Mr Wright: I think it is more than anecdotal. Certainly the British Crime Survey showed, when it asked people about viruses and malicious emails, that reporting to anybody was low and reporting to the police was even lower. So I think it is stronger than anecdotal. In terms of encouraging reporting, we have not done an enormous amount. We have done more work around awareness, around IT security issues and the role of the police, but we have not done anything particularly to encourage reporting. There is an online police reporting portal which allows you to report minor crimes, but again we have not done much to encourage reporting from individuals.
Lord Young of Graffham: How do you define e-crime?
Lord Howie of Troon: I was just going to ask that!

Q4 ***Lord Young of Graffham:*** The reason I ask is because you define it by way of financial loss, but frankly if a virus comes in and wipes my hard drive, that could cost me far more money than being mugged in the street?
Mr Wright: I was going to ask the Committee the same question, actually!

Q5 ***Lord Young of Graffham:*** I got in first!
Mr Wright: Let me say two things. One is, a lot of people spend a lot of time trying to define e-crime and come up with variations on the same themes. There is no great magic to it and I do not think it helps to get hung up about it, but when we talk about e-crime we mean any form of crime which is committed either using the Internet or using computers as an important tool. So a drug trafficker who sends emails, that is still drug trafficking, but actually a fraud where the initial contact between the fraudster and the victim is electronic then I would regard that as e-crime. We have tried not to define e-crime or organised crime because you would spend a lot of time talking about what is in and what is out and it does not actually help you with the problem, I think.

Q6 ***Lord Young of Graffham:*** So over the last 25 years we have migrated from letters from Nigeria to emails from Nigeria, so at some point that transmuted into e-crime?
Mr Wright: According to my definition, yes, but it has always been fraud. It was fraud then and it is fraud now.

Q7 ***Chairman:*** Do you have any idea of the ratio between e-crime and conventional crime? Let me give you an example. Say somebody ended up in a very unsatisfactory eBay deal, maybe because they were ignorant of what they should do, and they lost several hundred pounds. My feeling is that they are probably far less likely to report that than somebody who was mugged or whose house was robbed, where they would almost certainly report it. Do you think that is the case?
Mr Wright: There are two questions. One is about the proportion of crime which is online rather than offline. It varies between the crime types is my view, and I think a lot of fraud is electronic based. Certainly access to child pornography is now virtually all electronic based. With other forms of crime the proportions are far lower. So I think it varies according to crime type, but we do not have clear figures as to the clear proportions for any of those. In terms of where somebody has lost money through eBay and do they report it, certainly the online market phenomenon has meant more and more people transacting directly with each other in an environment where it is more difficult to gauge trust. If you meet somebody around the back of a pub, well, you have a view as to how trustworthy they are. That is more difficult to form online, so there have been more person to person transactions. Some of those get reported and some of them do not. I think people do not report to the police because they do not always think the police can help. The desk sergeants are not always as keen to take those kinds of reports as possible and there is not always a clear geographic nexus, and actually some people who get ripped off on eBay—it is like

buying things around the back of the pub, sometimes people know what they are buying. It is not necessarily the same as buying from a high street shop.

Q8 ***Lord O'Neill of Clackmannan:*** Are you concerned about the reluctance of financial institutions to make a clean breast, you might say, of the amount of incidents they have? We all know, for example, with credit cards you have a degree of protection and therefore there is maybe only a hundred pounds at risk, therefore it is not very much, but nevertheless is it crime. Are you happy with the amount of information which is provided by the financial institutions, whose probity or security might be undermined if they were unduly frank about their losses?
Mr Wright: The National High Tech Crime Unit and SOCA have very close relationships with the banking sector and have built up a relationship of trust and of information sharing and confidentiality, and I think they have strong relationships and there is a lot of information sharing, and there have been some notable operational successes off the back of that.

Q9 ***Lord O'Neill of Clackmannan:*** But that does not make the public records any more robust, does it?
Mr Wright: No, it does not.
Mr Webb: I think APACS, the Association of Payment and Clearing Services is the main forum there by which the industry reports these sorts of data and that is definitely one of the better data sources in the fraud area. The Government's Fraud Review noted the problem of under-reporting of fraud compared with other kinds of crimes, and I think that applies every bit as much in the e-crime area as it does for other sorts of fraud. So the financial sector, the card fraud data and the data we are getting on online banking fraud is probably some of the better fraud data that is out there.

Q10 ***Lord Sutherland of Houndwood:*** Presumably in the case of e-crime you are more dependent upon the victim reporting it, because if it is not an e-crime there could be independent witnesses but in the case of e-crime somebody has got to own up and say "this happened to me through this particular route," and that is bound to affect the statistics?
Mr Wright: I do see your point, but I think the surrogate for independent witnesses is either transactions through payment mechanisms or through ISPs. If one person reports and you do an investigation, then the police try to trace the individual and they find hundreds of other victims. I am not sure the analogy quite works, but I think to get it electronically—

Q11 ***Lord Sutherland of Houndwood:*** The first step has to be somebody saying, "I was cheated through this"—
Mr Wright: Yes, but once you have got that you could find many other victims in a way that you cannot offline, so yes and no, I think.

Q12 ***Lord Young of Graffham:*** Whilst we are on online banking and fraud, your memorandum said that online banking fraud went up by no less than 90 per cent between 2004 and 2005. I assume, in the absence of anything else, it is probably continuing to increase now. First of all, why do you think it is going up? Are there any defects in the systems? Secondly, how much longer can this continue to rise before you undermine the very basis of online banking?
Mr Webb: Again, this is an area where we have been working quite closely with APACS and the financial sector and it is certainly an area they are keeping a very close eye on. The absolute levels of losses are still a small proportion of their losses are their card losses, for example, still less than five per cent, but it is a very sharp increase. A lot of this is probably attributable to being reasonably in step to the actual amount of Internet banking. Over the same period we have had probably a one-third increase in the number of Internet banking customers. The financial sector is not able to work out by transaction which of them were done on the Internet and which were through other means because it goes through the same clearing system, but it is probable that the individuals are using their Internet banking side more. So a lot of this is attributable to the fact that there is more Internet banking going on and the fraud is not necessarily rising as a proportion of that, but it is something which we in the financial sector look at and there are ideas for additional security. Obviously the financial sector has just invested in chip-and-PIN, a £1 billion programme which has just come to an end and is already having an increase on certain sorts of frauds. Probably there has been a certain amount of displacement from that into this area because the fraudsters are determined to make their profits somewhere.

Q13 ***Lord Howie of Troon:*** Did you say that the apparently large increase from a small base was rather like—you remember Jonathan Swift talking about the man who made two blades of grass grow where one did before, which is an increase of 100 per cent, but it is really not very much? Is that what you are telling us?
Mr Webb: No. There are two things. First, we are saying that relative to the overall scales of losses to the banking industry this is still relatively small, but obviously the rate of growth is very striking. But

you also have to look at the rate of growth relative to the overall size of the industry. If the industry is growing at a huge rate, it would suggest that fraud as a proportion is relatively stable. We are not quite sure of our statistics, but certainly a lot of that increase is probably explained by the huge expansion in the amount of use.

Q14 ***Lord Howie of Troon:*** So you expect the 90 per cent increase to reduce year after year—if you are lucky?
Mr Webb: It is hard to tell. You have got 16 million customers at the moment. You would not expect the expansion to continue at quite the same rate and the number of people who have been going over to broadband, which makes these sorts of services easier to access, has clearly been a factor and at some stage that is going to plateau. The industry is going to keep a very close eye, and as are we, on the scale of losses and what countermeasures we need.

Q15 ***Lord Young of Graffham:*** Could I just follow up on that? If there is online banking fraud you would expect the customer to complain if £20 was taken out of his account, or whatever. Do you think the same person would complain because he bought something on the Internet for £10 or £20 which was never delivered? In other words, is there a threshold under which people will just not be bothered to go to the police and write it off as a bad experience, whereas with online banking they will?
Mr Webb: I suspect with online banking they would have that much more confidence that they would get redress from the bank, so they would report it first to the bank, and that is why this very often happens.
Mr Wright: I do not think there is a threshold, but I think people traditionally weigh up whether to report a crime to the police or not very carefully. There is the time and the trouble and what you get back, and if they see no likelihood of getting their money back lots of people do not report it. Things like insurance claims require a police crime number, which has driven up reporting.

Q16 ***Lord Young of Graffham:*** So there could be quite a lot of low level crime? If somebody buys dodgy goods on the Internet which never get delivered and he never complains, things of that sort?
Mr Webb: Yes.

Q17 ***Lord Sutherland of Houndwood:*** I would like to put to you two suggestions which have been put to us which have been related. The first is that there is a lack of effective legal sanctions to prevent the abuse of personal data, and the second suggestion following from that is that as a consequence London has become a base for international phishing expeditions and that sort of crime? These are two, as I say, linked suggestions put to us. Could I have your comments?
Mr Webb: If I could take them in reverse order. We are not aware that London is seen as a particularly large centre for these kinds of attacks. It is not something we, or SOCA or the City of London Police (Fraud) recognise, and it is not something we are hearing from our international partners, that many of the problems appear to be coming from the UK. Similarly, some of the frauds are going to be as a result of the misuse of data and some are going to be the result of other means of deception. The Information Commissioner, as you know, published a consultation paper called What Price Privacy? which has been consulted on by the Department for Constitutional Affairs. The consultation period has finished and they are now considering the responses, which have been generally very positive. So the DCA will be considering what to do and will need a legislative vehicle to increase the penalties in Section 55 of the Data Protection Act. That is something which is certainly under active consideration at the moment. We have not seen any evidence of a particular link between the sorts of Internet e-banking frauds we are talking about and this particular abuse of data. With phishing attacks, for example, the modus operandi would be rather different.

Q18 ***Lord Sutherland of Houndwood:*** Yes, but I take it from the way in which you have answered the question that there is a real issue about the effect of sanctions on the abuse of data, and indeed the Commissioner in the report you referred to suggested a minimum two year sentence for certain crimes in this area. Is the Government going to take that on board?
Mr Webb: As I say, it is a matter for the Department of Constitutional Affairs, which leads on the Data Protection Act. The Commissioner has certainly made a powerful case and the responses to the DCA's consultation exercise, I understand, have been generally supportive.

Q19 ***Lord Sutherland of Houndwood:*** Is there a timescale on that?
Mr Webb: I would not be able to comment on that. I do not know.

Q20 ***Baroness Sharp of Guildford:*** A couple of years ago the Home Office was working on an e-crime strategy, which I gather was due to appear in 2005, but equally in your memorandum there has been no mention of it. What has happened to it?

Mr Wright: That is true. We are actively pursuing a strategy to strengthen our response to e-crime, including the data about e-crime, which we have already touched upon, legislation, policing, international co-operation and prevention. Over that period of time we have created SOCA and the SOCA e-crime Directorate with responsibility for reducing the harm caused to the UK by technology-based crime. We have created a Child Exploitation and Online Protection Centre, whose remit is around working in partnership to protect children and society from paedophiles and sex offenders, particularly those who use the Internet.[1] We have negotiated an EU framework decision on attacks against information systems and implemented that and strengthened the Computer Misuse Act, and we have made good progress towards ratifying the Council of Europe Cybercrime Convention. Through the Get Safe Online campaign we have put in place a partnership between government, industry and law enforcement to provide good awareness information to the general public to try and reduce its vulnerability to this. We have worked closely with the IWF, UK ISPs, search engines and others to develop technical solutions to make it harder for UK residents to access child pornography websites. We have worked with SOCA and through the G8 contact network which involves 45 other countries to strengthen international co-operation. We ran at least one international event during our presidency of the EU and G8 last year and have put in place a virtual global taskforce to start to bring together law enforcement agencies to protect children as they use the Internet worldwide. As part of its work to develop control strategies to reduce the harm caused to the UK by all crime, SOCA has established a national e-crime strategy group to bring together the relevant government and agency players to develop a common approach and strategy towards tackling e-crime. We have not published a strategy, but we have made real progress in implementing a strategy over the last couple of years based on some of our consultation with stakeholders and we are now working with SOCA and the agencies to develop a new strategy to fit the climate as it currently stands.

Q21 ***Baroness Sharp of Guildford:*** Yes. You have not exactly been idle, have you?
Mr Wright: That was the point I was trying to make, at length.
Baroness Sharp of Guildford: Yes. Thank you.

[1] We have also strengthened the capacity of local police forces to respond to e-crime, as well as providing them with central training and guidance.

Q22 ***Lord O'Neill of Clackmannan:*** You have indicated that steps have been taken, that the National High Tech Crime Unit has been set aside and SOCA has taken over. Is there not a danger that you are going to be concentrating on high level e-crime and that other equally irritating petty crime will fall through the SOCA net because it is not big enough for them to deal with? What consolation can you give the citizen who is ripped off on a small scale?
Mr Webb: Over recent years, as Tim described, the National High Tech Crime Unit looked at the particularly major players, but at the same time we have been trying to build capacity with ACPO and local forces through computer crime units, through training and development for specialist police officers in this area. So we have been trying to build capacity at local forces, build capacity at SOCA and there has been discussion for some time about this gap at what is known as level 2, the sort of mid-level serious organised crime, and that has been identified in the O'Connor Report on protective services. That is something again we are working on with ACPO and APA to seek to address. The e-crime team in SOCA has a very similar remit to the National High Tech Crime Unit in that it is focusing on the high level and most serious groups, and nothing has changed there; indeed, the SOCA e-crime team has more staff than the NHTCU. It is actually strengthened. Far from having been disbanded, it has been expanded and strengthened.

Q23 ***Lord O'Neill of Clackmannan:*** Can I just be specific here? As far as level 2 crime is concerned, that is not a high priority at the moment for SOCA and there is a gap in policing in relation to level 2 crime? Would it be correct to say that?
Mr Webb: There are gaps in the protective services which have been recognised by HMIC and we are working to deal with that. Obviously SOCA is focusing on the most serious threat to the country, national and international crime, although SOCA has made it clear that ten per cent of its total effort will be assisting local forces. So there will be some capacity building, some technology and knowledge transfer, and so on, but nonetheless those resources are obviously limited.
Mr Wright: In terms of local forces and e-crime, I think since 2001 every force now has a Computer Crime Unit. They have grown significantly in strength over that time. We have provided through the Central Police Training and Development Authority a number of courses for both specialist and for all police officers to take up, to increase skills and knowledge both in the specialist units and in day to day policing, and we have provided guidance on how to manage force Computer Crime

Units. So it is getting better but, as Stephen says, there is a gap in how forces deal with level 2 crime across all types of crime and e-crime is a subset of that.

Q24 ***Lord O'Neill of Clackmannan:*** Is that a constraint of physical resource in terms of human gains or financial resource which is preventing you from expanding?
Mr Webb: The HMIC Report looked at a lot of factors, the critical mass in some forces, the increasing specialisation of some tasks (and obviously e-crime would be a particularly good example of that), the difficulty of co-ordinating across border boundaries. As I say, a lot of work is going on with ways of addressing that.
Lord O'Neill of Clackmannan: Thank you.

Q25 ***Lord Howie of Troon:*** Earlier on Lord Young here asked if there was a definition of e-crime and I am not sure that he got a terribly clear answer to that question! This leads me to ask, how many people are being prosecuted for e-crime, or are they lumped in under things like fraud and so on? If you could clear that up for me because I am in some confusion there.
Mr Wright: It is very much the latter. Not only do the police databases not distinguish between whether crimes are committed electronically or not, but nor do the Prosecution or the Home Office figures distinguish between the two. So we do not know how many people have been prosecuted for e-crimes as distinct from offline crimes.

Q26 ***Lord Howie of Troon:*** So is it easy to find appropriate offences to charge them with?
Mr Wright: I think the corollary of not distinguishing is that actually it is easier to find charges because it is fraud, it is theft or it is extortion, however you commit it. We spent a lot of time talking to the CPS and investigators to identify gaps in the criminal law and to see whether there are people they cannot prosecute where there has clearly been criminality and where we find gaps we try and plug them, for example the Computer Misuse Act, which we have strengthened, and the Fraud Act (as it is now). By and large, the practitioners tell us the problem is not finding offences, it is having enough evidence to prove the offences which is the difficult bit. So no, we do not think there are gaps in the framework.
Lord Howie of Troon: This is beginning to lead me to wonder if e-crime actually exists!

Q27 ***Lord Young of Graffham:*** Would it not be of advantage for the police records to at least show the number of cases in which the Internet was used? It is like keeping road statistics and not distinguishing between drunken driving and speeding. You have got to have some idea which crime is increasing or not.
Mr Wright: Yes, I think is the short answer to that. There is always a tension between collecting more data and actually using it, but I think in this instance our view and ACPO's view in the past has been that we need to be able to understand what balance of crimes are online and offline to inform (a) how we tackle it, and (b) resourcing and managing both performance and resourcing around that. It is something which is not in place in many forces. It is something which we and ACPO have been working on and I know the ACPO lead on this issue is talking to colleagues about this again.

Q28 ***Lord Howie of Troon:*** With some other offences the word "aggravated" is used to define a specific subspecies of the offence. Would you expect something of this sort to be done, fraud aggravated by e-crime, or something? Would that be even remotely sensible?
Mr Webb: It is not obvious why it would be an aggravating factor. The Sentencing Guidelines Council and Sentencing Advisory Panel have looked into "seriousness" and what should be seen as potentially aggravating factors, and there is quite a recognised list across the board. You have to make a case for why it was worse to defraud someone over the Internet rather than sending them the 419 letter by post, or scamming them and meeting them face to face on the street.
Mr Hendon: Perhaps the value of having a term like e-crime is that it draws attention to the potential victims that they may have a crime committed against them in a place where they would not have previously expected that crime to take place, so they are not safe when they are sitting at home with their computers against e-crime, although it is probably fairly safe that they will not be defrauded in the conventional sense.

Q29 ***Lord Howie of Troon:*** Yes. If you are mugged you would probably notice!
Mr Hendon: You might do, yes. Perhaps it is as much about it is useful to raise awareness as anything else. Probably it is not particularly useful from the prosecution point of view.
Lord Howie of Troon: Thank you.

Q30 ***Chairman:*** In all likelihood you are being defrauded by somebody who is not even in this country?
Mr Webb: That is quite possible, yes.

Q31 ***Chairman:*** So what are the possibilities of dealing with criminals in other jurisdictions?
Mr Wright: Obviously it is harder to deal with a criminal outside the jurisdiction than it is inside the jurisdiction. The UK has a very good track record of bilateral co-operation with other countries' law enforcement agencies, I think probably better than many other countries. We work actively through Interpol, through Europol, through the G8, through their contact network of Computer Crime Units, but also bilaterally. The National High Tech Crime Unit spent a lot of time building contacts directly, many of which have paid off, and again part of the *raison d'être* or one of the benefits of creating SOCA is that lots of crime is becoming increasingly international and SOCA will be a powerful vehicle for UK law enforcement in co-operating with colleagues overseas. The point is, we have had a lot of good results in targeting serious organised criminal groups out of the jurisdiction. That is not to pretend it is easier to deal with people overseas than it is here.

Q32 ***Chairman:*** So do you think it is a possibility that we could have an international e-crime police force?
Mr Wright: As I have said, the way we have approached this is to build and strengthen our relationships both bilaterally and multilaterally with other countries. We have not actively considered the creation of a global or international police force as a separate entity. I think there is a number of issues around resourcing, jurisdiction and around political clout which would distract us from actually getting on. What we have done, on the child protection side for example, is create a virtual global task force to bring together, at the moment only us, America, Canada, Australia and Interpol, but they are people who work for national law enforcement and they work closely together on reporting, on sharing intelligence and on preventative operations, but they do that from within their own national force. I think in the short term exploring that kind of avenue for closer working between national forces is a much quicker way of making progress.
Mr Smith: Can I add, my Lord Chairman, I think we should also look at the international collaboration around the prevention of crime. I personally think that the idea of an international police force in this area is a long way off, but the banking community is actively working throughout the world to stop the phishing attacks having an impact. At the moment they are actually being very successful in cutting off the websites which host these attacks and the flow of money which arises from the attacks. So in terms of prevention, I think there is developing international collaboration both in the communications provider area and in the financial services area, so there are two sides to this question.

Q33 ***Lord Sutherland of Houndwood:*** I was going to ask a couple of questions in this area which I think will follow naturally from the discussion we have just had. One is a very straightforward one. You mentioned some of the examples. Are the structures adequate for dealing with international colleagues? Secondly, do they fit all of your potential partners equally well? Some countries might be more co-operative than others. What are the personal relationships like? Can you phone people up and get a quick response?
Mr Wright: In reverse order, the personal relationships between law enforcement officers I think are excellent—

Q34 ***Lord Sutherland of Houndwood:*** In all countries?
Mr Wright: No, to be absolutely honest.

Q35 ***Lord Sutherland of Houndwood:*** I am not going to ask you for a list!
Mr Wright: Again, I am speaking second-hand, but if I can go back a point, the UK is better at building those relationships than pretty much anybody else I can think of and it works in terms of the operations we have had, good co-operation and good results, and we have been able to help other countries, but a lot of that is about personal relationships. Interpol exists as a global framework, 150-odd countries,[2] to share intelligence and co-operation. On computer crime there is a separate Interpol group and there is a G8 network of Computer Crime Units which has about 45 countries and we got over half of them together a month ago in Rome to do a training conference, to try and build those relationships and on a practical level help people co-operate. I think the structures are okay, and actually there are some things we need to do bilaterally and will not want to do in a multilateral forum. So I think from a UK perspective it could always be better and international co-operation is difficult, but we are doing as well as anybody could expect.

Q36 ***Lord Sutherland of Houndwood:*** Are you sufficiently confident across the board that you can share information securely? [Pause] I think you have just answered the question!
Mr Wright: Yes, but I think through traditional means. I think we share things securely, but through traditional means.

[2] 186 countries

Q37 ***Lord Sutherland of Houndwood:*** Just a last detailed question. Are there examples where folks overseas would say, "That was marvellous. The Brits did very well"? In other words, have there been prosecutions from abroad of UK residents, the UK-based?
Mr Wright: There have been prosecutions of UK residents either under UK law or where people have been or are in the process of being extradited, and we are able to co-operate and support other people.
Mr Webb: There was a couple of hackers causing considerable damage in the United States.
Lord Sutherland of Houndwood: Yes, I remember that case.

Q38 ***Lord Patel:*** I have a series of linked questions. The first one is that the Get Safe Online survey suggested that the consumers felt more at risk of Internet crime than they are of being mugged or robbed. Do you think their perception is wrong?
Mr Smith: I think we were all surprised by that result. It does seem counter-intuitive and I think perhaps we need to look a bit more closely at that questionnaire before it is re-run, but it was run by a legitimate market research company and I think it had a response rate of around 300. I am not sure how the respondents were selected, but I think many of us involved in the Get Safe Online campaign felt a bit uneasy about using that as our headline message, but that is what the survey showed.

Q39 ***Lord Patel:*** If that was the public's perception, how effective has the campaign Get Safe Online been?
Mr Smith: I think it is a very good campaign. I have actually asked the organisers of the campaign to send you a DVD of the recent campaign, which I think gives a flavour of how it worked and how it was received. I think if you look at the number of links to the sites, the number of hits to the sites, it was an incredibly successful campaign given the relatively small amount of money which was expended on it. The market research actually does try and measure its impact and it has found a very high degree, I think 33 per cent of respondents claimed to recognise the Get Safe Online brand, and that it was starting to have a real impact on consumer behaviour. It is, as you say, linked to some of the earlier questions because I think the phishing attacks would disappear overnight if people did not give out their personal information in response to an email from a bank, and if Get Safe Online can get that message across, if the APACS anti-phishing campaign can get that message across, then that form of Internet fraud will wither and die. I think if the Get Safe Online was getting those basic messages across, "Don't give personal information out over the Internet. Be careful what sites you visit. If you click on a link from an unknown or untrusted source, you will probably be downloading malware. Keep your antivirus up to date. Patch your system," those basic, if you like, hygiene issues that consumers need to do to protect themselves then I think it was successful in those terms.

Q40 ***Lord Patel:*** Do you think the Police Forces have enough staff with the necessary skills to carry out a forensic examination of IT crime?
Mr Wright: Police Forces can always use extra staff for any discipline. As I said earlier, every force has a forensics unit. They have grown significantly over the last three or four years. ACPO are currently surveying the capability and the capacity of those units to see whether they are up to strength. My guess is that they could easily absorb quite a lot of extra investment.

Q41 ***Lord Patel:*** Do they have targets for the policing of e-crime?
Mr Webb: No, there are no such targets, and I think that relates back to the sort of discussion we were having earlier about defining ecrime. If you do not have any clear agreed definition, it would be quite hard to do targets. In addition, we are generally in an environment where the Police Forces and the police authorities are looking to reduce the number of central targets we impose as part of releasing bureaucracy and freeing themselves up to dedicate themselves and dedicate the resources in the way which seems best for them for national and local priorities. So there are no targets because, as Tim was saying earlier, generally we see this as another way of carrying out similar crimes, many of which are obviously covered by PSA targets for crime reduction.
Mr Wright: That said, we are working with ACPO and HMIC to develop measures specific to that capability, to go into every force's baseline inspection. We will know more clearly in the future.

Q42 ***Lord Patel:*** So the police would investigate any reported e-crimes?
Mr Wright: When people report crime, it is the job of the police to investigate. What I am saying is that we are working with HMIC to set inspection measures so that when HMIC inspect forces they will be able to say, "How big is your forensics unit? Is it keeping up or is it not keeping up?"

Q43 ***Lord Patel:*** So is the Government putting in extra resources?
Mr Webb: Generally this is an area where what we have done over recent years is to provide a certain amount of pump priming funding, but broadly

speaking because it is a crime like any other we would expect it to be covered by the police grant. There has been a very substantial 45 per cent real increase in overall funding over recent years, so we would expect it to be covered by the standard police grant and precept.

Mr Wright: Ministers announced yesterday a seven per cent[3] increase from this year to next year in police funding as well.

Lord Patel: Thank you.

Q44 ***Lord Young of Graffham:*** Looking internationally for a moment, what are the main black spots around the world for e-crime, assuming we can define e-crime sufficiently? If you do define such areas—and I will take one example only because it is fairly well public, Nigeria and the things which emanate from there—what sanctions do we have, or could we have, or should we have to reduce that, not just a virus but all the sorts of things which come, virus attacks, phishing, and everything else?

Mr Wright: There are specific nationalities—and I think we often talk about nationalities rather than countries because people move around—more strongly associated with e-crime than others. The ones which come up a lot are the Chinese, Brazilian, Russian and the former Eastern Bloc. As you say, we are identifying Nigeria as well now. Our response has been to engage with local law enforcement in those countries, either to run joint operations or to help by providing either assistance or support in being able to tackle some of these people on their own patch. On the question about sanctions, we do not have sanctions we can apply to countries at that kind of level.

Q45 ***Lord Young of Graffham:*** Should we have some form of international agreement in which we can make some nations look after their own people better, or restrain them more?

Mr Wright: I think the only big international agreement in this field is the Council of Europe Cybercrime Convention, which requires all parties—and they go way beyond Europe—to have robust legislation procedurally, which means extracting data and being able to extradite people, as well as offences, but that does not go as far as one country being able to act against another. I think that would be an enormous step in international law for us.

Q46 ***Lord Young of Graffham:*** So whatever in effect we can do about e-crime in this country, since the Internet is global we are not going to do anything powerful. We do not have the tools to do anything to stop it emanating from other parts of the world?

Mr Wright: I think it is working, particularly law enforcement but also with government and industry in other countries, and we work closely with the agencies in those countries. I am not sure it is appropriate for the UK to do directly things in other countries, but what we do is we work with the institutions available in those countries, mainly law enforcement, often with governments and with the agencies. I think there are some signs of success in this, but it is trying to fit national jurisdictions and frameworks on an international crime problem and that is never going to be entirely straightforward, and it applies to all crime, not just to e-crime. Obviously, it is more a factor in e-crime than it is in most crimes and there is a lot of international crime. A lot of crime is cross-border, drug trafficking for one.

Q47 ***Lord Young of Graffham:*** Yes, but if you are running drugs you have to deliver them from one place to another and there are physical ways in which you can stop this. Here it is almost impossible, is it not?

Mr Webb: It really has brought international co-operation to a whole new level of importance in a crime area which previously would have been probably within the jurisdiction and has now suddenly become international, even with frauds and crimes which are relatively small in value, and it is one of our big challenges.

Q48 ***Lord Young of Graffham:*** Are there any recommendations we should be making about looking at this particular area, because it always does seem to me of considerable concern because you can get small jurisdictions which can inflict considerable damage and you have very few sanctions against them?

Mr Wright: Yes, and I think there is a risk that the brighter criminals will move some of their criminal operations to the jurisdiction in which they perceive the risk to be lowest. In terms of recommendations, I am not sure there is anything beyond our current approach that we would encourage you to recommend, but I am not sure it is for us to recommend what you recommend to us.

Mr Webb: We want to work closely with SOCA and other law enforcement agencies to get a feel for where the problems are with international co-operation. Ministerially we have certain levers, we have international organisations where these matters can be raised, and we really want to work with our law enforcement colleagues and get them to identify the problems they are having. At the moment we have not got a feel for anything specific, but it is something we are very keenly aware of.

[3] 6.9 per cent.

Mr Wright: There is more we can do in terms of working with industry. Many chunks of this industry are multi-national anyway and I think there is more we can do in working with industry.

Q49 ***Lord Young of Graffham:*** The problem is, if we are going to rely on the other jurisdictions to control themselves—I mean, it is alleged in some parts of the world that the drug interests have taken over the governments of small nations and you could see organised crime taking over small jurisdictions and they are finding it very difficult to deal with this since the Internet gives you total access everywhere?
Mr Hendon: I think one of the problems is that it can be very much easier to move your source of crime to another jurisdiction. It is very much quicker to do that than it would be to set up a new collaboration with that jurisdiction to get rid of it. So basically we have to solve these things here, I think.
Lord Young of Graffham: Yes, that is right.

Q50 ***Lord Howie of Troon:*** You mentioned the Council of Europe. Would you remind me, as I have clearly forgotten, are pronouncements and recommendations from the Council of Europe mandatory?
Mr Wright: Yes, I think that is right.
Mr Webb: For those who sign up to the Convention they commit themselves to implementing them, yes.

Q51 ***Lord Howie of Troon:*** Do they really?
Mr Webb: We may be stretching our Constitutional knowledge!

Q52 ***Lord Sutherland of Houndwood:*** The question is, do they really commit themselves?
Mr Wright: That is right, and we have not ratified the Council of Europe Convention on Cyber Crime from 2001 yet. We are close to having implemented it, but the UK has not ratified it yet, so we are not in a strong position to comment on other people.

Q53 ***Lord Howie of Troon:*** I think that really is a virtue!
Mr Webb: What these conventions generally require you to do is to change the law but what they do not necessarily tell you is how much effort is then being put into tackling the problem.

Q54 ***Baroness Sharp of Guildford:*** I take it from what you are saying that if all the main players in this signed up then safe havens of one sort or another would appear?
Mr Wright: I think it is always a risk and it is not just legislation, it is really enforcement.

Q55 ***Chairman:*** It strikes me that the one thing which could be done is to insist somehow internationally that email addresses, et cetera, were identified with their physical location. That is not the case at the moment because if you get an AOL account or anything then it becomes invisible as to where you come from. Regulations could be set, I would have thought, on the Internet to insist upon it, so if you saw it coming from a certain country where you knew you had no interest whatever, nor expecting anything, then you could reject it. The thing which personally annoys me is that you have absolutely no idea where this email is coming from.
Mr Smith: That is true, and I think there have been discussions over several years in the Internet Engineering Task Force and elsewhere about the possibility of identifying the source of email traffic. Those discussions are ongoing. I think it has been driven largely by the problem of spam, where I think the solution would be greatly alleviated by having a system whereby you can identify the origin of the email. There are other solutions being discussed. I think this is a very relevant point. It is not something which the UK Government could in any way mandate by itself, I think it actually needs the industry to come together to find a common solution. So we are looking at multilateral organisations like the Internet Engineering Task Force to come up with solutions, or for large companies to come up with solutions.

Q56 ***Chairman:*** But if this happened we would be advocates for something being done, would we?
Mr Smith: Absolutely. I think the whole problem of identity on the Internet, knowing who you are dealing with, is a key issue not only for preventing e-crime but also promoting e-government and e-commerce. I think one of the big areas of debate which is taking off at the moment is identity as the Internet becomes more ubiquitous, how we are going to identify ourselves to other individuals, indeed to other machines. I think we are at the start of the debate.
Mr Hendon: But it also requires that the identity is real, and so you get into the whole question of how you can be sure that people are who they say they are and that they are related to the place or the organisation, or whatever it is, which is leading you to think they are someone you want to talk to. So I think it is quite complicated to see how to make it work.

Q57 ***Chairman:*** Let me go on and ask you a question about Europe. What interaction is there between the UK and the European Network and Information Security Agency (ENISA) and when will the UK

ratify the Council of Europe Convention on Cybercrime which was signed in 2001?

Mr Smith: Shall I take the ENISA question first? I cannot really talk for the UK but I can talk for myself. I am the UK's board member on the European Network and Information Security Agency, so I have been playing a very active role in getting the agency off the ground and getting the first two work programmes completed. The UK also participates at the level of national liaison officers where the agency has created contact points with each Member State. I think we have been very fortunate in having a strong contribution on the Permanent Stakeholder Group, who are stakeholders who have an interest in the work of the agency. We have got the largest single number of members and some very good people are working with the agency to try and give the work programme focus. So I think the UK has been a key player and I think in the work that we have seen the agency doing on Computer Emergency Response Teams (that is a way of dealing with real-time issues) and risk management, the UK has made a major contribution, but particularly, I think in this context awareness raising, getting the message across to all stakeholders about the importance of taking the right actions. There has been some useful dialogue at the European level and the UK has made a significant contribution to that dialogue, drawing on its experience with Get Safe Online and other consumer campaigns. So I think we are actually one of the leading Member States contributing to the agency. You have to remember it is a very small agency, so we have very limited expectations of it, but I think it can make a useful contribution in creating networks and disseminating best practice amongst administrations.

Mr Wright: In terms of the Council of Europe Cybercrime Convention, we cannot ratify until we have implemented all the provisions, which touch on a number of pieces of legislation, pretty much the last two of which are the Fraud Act and the changes to the Computer Misuse Act in the Police and Justice Act, both of which got Royal Assent this month. Once we implement those provisions, we should be very close to being able to ratify.

Chairman: Thank you.

Q58 ***Baroness Sharp of Guildford:*** What is your assessment of the current level and impact of email spam on individual users and the economy as a whole, and what is the Government doing about this particular problem?

Mr Hendon: Perhaps I can take that question. It is extremely difficult to assess the current level and impact of spam. It is clear there is an enormous amount of email traffic which is spam. I hear figures for big organisations that perhaps half of the emails which come into their files are spam. When you try to pin down the impact in numbers, then no one seems to agree and it is very hard to find any number which is more convincing than another. I thought it is quite interesting that the EU has just put out a communication on spam, spyware and malicious software just last week and in there they say that the impact on the UK is €1.9 billion in 2005, which sounds like quite a big number, and when you look to see where they got that information from, it says "various sources," which I think really makes the point that actually they are not going to pin it down either. So I think it is extremely difficult to assess. Obviously spam which is simply suggesting you might like to buy drugs, Viagra or something, or to buy shares in some start-up in the US which no one has ever heard of are not particularly damaging if they simply get deleted at the point they happen, but if they include a link to a phishing site and it leads you to lose money, then of course the impact is very much greater. So it is very hard to pin it down and I think we simply do not know the answer. It is clear it is a big problem and something needs to happen, but it is very unclear exactly the level of the impact. What are we doing about it? We have actually had quite a sort of leadership role, I think, internationally from the DTI and one of my officials in particular over the last few years has been very active in bringing together international co-operation around spam. The London Action Plan, so called, is an international grouping of a number of different countries and organisations within the countries, all working to a set of agreed rules and procedures. The sorts of things which were going on there led to work which was done in the context of the OECD and there is an anti-spam toolkit. This toolkit, if you look at it, has a whole set of things which a country needs to do in order to get itself into a better position in relation to spam. If they follow all the rules in the 100 or so pages of the toolkit then they will sort the problem out for themselves. Then most recently at the Internet Governance Forum in Athens last month the Stop Spam Alliance was formed, which brought together about six of these international groupings and I am glad to say that my official was chairing the workshop which made that happen. So we really feel that although in some ways it is a small amount of money to pay for one official to do this part time, nevertheless it shows what you can achieve if you actually focus it in the right place.

Q59 ***Baroness Sharp of Guildford:*** Yes. Sometimes it is suggested that it is illegal to actually block spam or for the ISPs to scan customer machines for insecurities. Is that actually so, and if so are there any plans to change the law in that area?

Mr Smith: There have been discussions amongst lawyers in the Internet Service Provider community about that and I would say it has not been tested in court. Our experience is that nearly every Internet Service Provider is filtering spam at the network level, and indeed I think the much reduced impact of spam on individuals in boxes is as a result of that network filtering. As I say, it is not tested in court. You can see analogies with tampering with the mail, but I certainly do not think anyone believes they are taking a risk in doing this. So they must have fairly strong legal advice that they are on the right side of the law.
Mr Webb: If any spammer identified himself and wanted to take his case, some other people might have something to say to him in return!
Baroness Sharp of Guildford: Yes. Thank you very much.

Q60 ***Chairman:*** I think this problem is really quite serious and our specialist adviser, Dr Richard Clayton, has just pointed out to me that he is familiar with one large ISP which in May was receiving 6 million emails a day and now they are receiving 26 million emails a day, of which 90 per cent are spam. It is the filtering in the major centres which is saving individuals. So, you know, businesses can deal with it, but if you are an individual user the increase in the last two to three months has been staggering. There is something going on.
Mr Smith: I think Dr Clayton knows more about this than I do. You see an enormous number of estimates of spam. Symantec, which is a large US security company, has recently estimated 54 per cent of traffic, but I saw an estimate this morning from a company I had not been previously aware of, of 90 per cent of traffic. Now, between 50 and 90, I guess it has got to be somewhere in there, but we know it is a large proportion of traffic. I had not heard that figure and that is an alarming increase if that is happening across the ISP community.

Q61 ***Chairman:*** Anecdotally, it would certainly match with my personal experience. I start now by eliminating three-quarters of the emails which have come in.
Mr Smith: I was going to come on to that. I think we have also seen over the last year the spammers getting cleverer and I think what we see in all the security issues is a race between the security solutions and the security problems. Now spammers have realised that the spam filters were reading the headers of the emails, so now they have got a way of generating random headers. They realised that they could spot a pattern in the body of the email at the filtering level, so now the spam communication is a picture and it is very difficult to filter out any email which has a picture attached. So you are actually on the up curve of getting email into your box, but we believe the industry will ultimately provide solutions to these problems.
Mr Hendon: I think one thing which makes me feel reasonably optimistic is that some of the commercial email providers are very effective at removing spam. For example, I have a Hotmail account which I use occasionally and very little spam actually gets through, and yet presumably there is a fair amount being filtered out. I guess if people in effect enter into a contract with their service provider which is about the service provider helping them to be safe—and I think there is an increasing interest in the service providers in bundling services to differentiate themselves and that keeping their customers safe is part of what they can offer—then this will make spam less useful to the spammers and hopefully it will die away.

Q62 ***Lord Howie of Troon:*** I am wondering about responsibility here. Who is responsible for the safety of the individual while online? Is it the individual's responsibility to protect himself, or is it the provider, or is it the Government in some way?
Mr Smith: I think certainly it is to a large extent the responsibility of the individual to behave responsibly. I think the Internet has grown so rapidly that we have not really developed safe behaviours around it. People grow up with an instinct about crossing the road safely but you do not yet have that instinct about using the Internet safely, and I think that is partly the responsibility of Government and business to get those kinds of messages across to create this culture of security. But essentially if you give out information over the Internet to someone you do not know, or you cannot be certain of their *vires* and then they take all the money out of your bank account, it is largely due to your behaviour and not the failure of the bank or a failure of the operating system, or whatever. So we have to get this message across that you need to proceed with caution, especially where money is concerned. I think it is fair to say that the service providers, the hardware manufacturers and the software producers all have a responsibility to improve their performance and if you read some of the material which was coming out of the European Commission it talks very much about increasing the responsibility of business in addressing these problems, and we would certainly support that. I think the question now is how we engage with business when that business is largely based outside of Europe to improve their performance. I think everyone is responsible, but let us not forget that the individual has to behave responsibly.

Q63 ***Lord Howie of Troon:*** In your evidence to us you said there had been a shift in people accepting that it is primarily their own responsibility to make sure they are safe when online. Does this mean you are really shifting the responsibility onto the individuals, who accept this because they get help from nowhere else?
Mr Smith: I would not have put it that way.

Q64 ***Lord Howie of Troon:*** I daresay!
Mr Smith: My view is that people have taken a rather rosy view of life on the Internet. It did have its origins in some fairly insecure and idealistic views of life, but now all of human life is on the Internet and I think people are beginning to become aware that there are villains out there who will take them for all they are worth. So I think what we were saying in our evidence was that we are detecting a greater awareness of the problems. Perhaps saying it is more dangerous or more worrying than mugging, is perhaps even more dramatic than we had expected, but certainly people are becoming more aware, and that is not an attempt by the Government to shift responsibility onto them. We want them to behave responsibly.

Q65 ***Lord Howie of Troon:*** Do you think it is a bit like putting up a burglar alarm at your home?
Mr Smith: Absolutely.
Mr Hendon: I think actually another analogy—and I am reminded of this by the mobile phone ringing—is that in Underground stations and in Underground trains now you see signs which say, "The best place to lose your phone is just outside an Underground station," because people come out and check to see if they have got a message and they get their phones taken away. So actually they are expected to change their behaviour when they check their phones, and that is what we are talking about here too.
Lord Howie of Troon: Yes. Thank you.

Q66 ***Lord Young of Graffham:*** Could you argue that the supply of an unprotected broadband line is not really fit for purpose and that the only broadbands they should provide are those which have a measure of virus and spam and other protections, because if you think it through you would not have a road which people were allowed to drive on, which was full of obstacles, or whatever? It does seem to me increasingly that broadband unprotected in any way at all is the quickest way to infect your computer. It is three or four hours, I think, for an unprotected machine on broadband to be infected by a virus, probably less?
Mr Smith: It is less than that, yes.

Q67 ***Lord Young of Graffham:*** I am declaring an interest. I have a company which does such things and they would hate me for saying this, but could you argue that providing broadband unprotected is really under the Trades Description Act not fit for purpose in some way?
Mr Hendon: I would not think you should argue that because I think it does depend what you are going to use broadband for. I think some of the new high speed applications, television, and so on, actually could be completely frustrated by the sort of computing overhead required to make checking happen. But if you turn it the other way round, you would not expect to walk down a motorway and not be run over, and actually if you are going to go on a motorway then you should be in a car and it should be fit for the purpose.

Q68 ***Baroness Sharp of Guildford:*** Yes, but using that analogy both in terms of safety and car theft, a lot of pressure upon the manufacturers to improve their product has actually made an enormous difference. If, for example, either those who sold computers were required to make sure that the software incorporated in it not only had the facility to incorporate the firewalls, and so forth, but actually had them up and running when they were sold and the price had to include this, this might make some difference?
Mr Hendon: There is a couple of problems I see with that. One is that the UK is part of the EU and so we at least have to take the rest of the EU with us before we could get away with that sort of restriction. I think a bigger problem actually than that is that today's solution is perhaps going to not be the solution tomorrow, because as soon as you block something then people who want to get through will find a way round and with the Internet the basic technology is designed to avoid people blocking it. That is where it originally came from. So actually what we need, I think, is a much more responsive reaction from the service providers in particular, who should be looking to work with their customers and with the people selling computers and software to be able to respond extremely quickly to things that people start to do. With the best will in the world, the Government is never going to be able to get the rest of the EU to come behind some sort of regulation or change of regulation to respond to something which suddenly starts to be the problem of today.
Chairman: Lord O'Neill, you have a question in and around this topic.

Q69 ***Lord O'Neill of Clackmannan:*** Yes. Very simply, there has been a lot of self-congratulation about self-regulation, but there are other areas where you would say really it is no longer enough to walk quietly with a big stick, you have actually got to use

the big stick. Nobody likes regulation, but there may well be areas of safety which need tightening up and where the UK, as a Member of the EU or through the Council of Europe, would wish to see things toughened up?

Mr Smith: I think, if I can add to the self-congratulation about self-regulation, I think it is very apposite to encourage self-regulation in such a dynamic area as the use of the Internet. The problems are changing overnight, literally. We see different problems nearly every week and I think traditionally the regulatory model does not fit easily with this kind of dynamic situation and with a business which is incredibly mobile. I think the prospect of losing business to more lenient regimes has to be accepted, so we have to move together within Europe and I think any UK attempt to regulate this in isolation would be foolhardy. There are no plans to introduce new regulation, apart from the ideas which are emerging in the context of the review of the communications regulatory framework. That is the framework which provides a common European approach to how telecoms and Internet Service Providers run their business, and there is a clear focus on security in the ideas emerging there. So we will be discussing regulation in that area. Similarly, the communication which has just come out around spam and mailware is talking about possible regulation on, I presume, Internet Service Providers to address this problem, but these are early days on those discussions. But I think it is difficult today to say there is a hard and fast case for regulation in that area.

Q70 ***Lord O'Neill of Clackmannan:*** We have the position at the moment in the UK where a number of ISPs are offering you a bundle of services, telephone, cable television, and the like, and that you are getting free broadband. Now, we know there is no such thing as free anything, but as a consequence of that what we are beginning to see is probably the paring down of some of the elements of the broadband service and as a consequence of that it may be at the price of insufficient regard to security. I have to say that the bundle we have at home is quite reassuring, but I do not know if it is across the board. Now, I wonder whether that is a case for regulation or whether you could be more insistent that within these bundled packages there would be appropriate and regularly updated security arrangements?

Mr Hendon: I think that actually this change is rather reassuring because what is going on is that these big companies are fighting each other for market share. They are trying to get customers off each other and hang onto them, and actually persuading people that if they take their bundle of services then they are going to be looked after or will be safe I think will be a very good product differentiator. Although the free broadband headline is the one which is selling right now, obviously we all know from talking to them that all they have done is re-partition the costs in a certain way. The bottom line is they have still got to maintain their market share and to keep the customers there, so I am not too concerned about that. If I could just add one thing to what Geoff was saying just now about regulation. Sitting listening, it struck me that it could sound a bit complacent, but actually what I would like to say is that there is a tremendous constructive tension between the Home Office and the DTI in this area of regulation because essentially they are trying to deliver the society benefits which the Government wants and we are trying to deliver the industrial competitiveness benefits the Government wants, and we talk together and we find some accommodation in the middle, which is where the Government goes. This accommodation is constantly reviewed, so although we are in a position where we believe self-regulation is better and we do not want to regulate, partly because we do not think it is going to be effective for very long, this is something where I could not say that even tomorrow we might not want to discuss it again. So I think it is something we will continue to keep under review.

Mr Smith: Can I also add that we are also in discussion with the ISP community about a new initiative. I am not sure one would describe it as self-regulation, but certainly to develop a better understanding of what ISPs can offer as, if you like, a minimum service or what we would see as a code of practice around the security they are offering to their consumers. It is early days, but again I think it is in response to this general expectation that the service providers should raise their game.

Q71 ***Lord Howie of Troon:*** We had some earlier experience of creative tension, I remember, between departments, notably the Treasury and the late Department of Economic Affairs. Is it always such a good idea?

Mr Hendon: I think I probably would not want to go as far as to say it is always a good idea, but to take the point seriously, there has been a similar creative tension between the Department for Trade and Industry and the Department for the Environment, Food and Rural Affairs over the chemicals regulation and the REACH regulation, which is not quite but almost put to bed, owes a lot to us discussing with Defra what was the right compromise between its environmental concerns and our industrial concerns. I think that is actually a good way for us to find the right answer.

Q72 ***Lord Howie of Troon:*** I hope you won!

Mr Hendon: I think we did okay.

Q73 ***Chairman:*** To finish up on this topic, could you comment on whether you think retailers of IT equipment should be obliged to demonstrate that their equipment is up to date and fit for purpose before it is sold? Should it have a sell by date on it?
Mr Smith: I have not come across that idea before. A sell by date on the actual hard drive?

Q74 ***Chairman:*** Well, it has to have antivirus software, for example, which is up to date.
Mr Smith: I understand. We do not actually monitor developments in the market to any great extent, but just observation would tell you that most manufacturers now are including basic software, operating system software and basic security software as part of the package. Most of the common software packages tell you pretty quickly that you need to update, so I am not actually sure—I suppose you could buy something, a 2004 version—
Chairman: A lot of PCs are sold without commercial antivirus and firewall software in them, I think. Anyway, let us move on because we are running out of time and we have a couple of questions which we really would like to get to. Lord Sutherland, you have a question.

Q75 ***Lord Sutherland of Houndwood:*** Yes, and it follows on very well to the point you have just made, because it has been suggested to us by children's charities that computers sold in this country perhaps should be sold with the assurance that they have a filtering product built into them and with a high default security setting as a complement. You can see why this is important. It presumably would not have to wait on European agreement because it is a product in this country and it is something this Government could do if it so chose. Is there a Government view on this?
Mr Smith: Yes, we have had the same discussions with the children's charities and they actually stated to us that there is evidence already of some of the larger manufacturers providing equipment with filtering software included. We are talking to those charities about how we might work together to encourage that, but for the reasons David described earlier, it is not something we think we could mandate, but again I think it could be an area of developing best practice to actually encourage the manufacturers.
Mr Wright: This is maybe a good example of the creative tension between our Departments because it is something we have worked on very closely. From our perspective, obviously this kind of software, parental control software, can help parents manage the way their children use the Internet and it is very useful. Obviously no product can be 100 per cent effective and no product is a substitute for parenting, and we have to say those things quite clearly to start off with. So we have been working with the British Standards Institute, Ofcom, the industry and the children's charities to deliver a standard for these products, because actually there are a lot of products out there which vary enormously in quality and when people say to us, "Do I need a product? Which product shall I buy," we say, "Products can help you and we are not prepared to recommend a product," and the quality varies. So we have been working on a kite mark standard and we are close to being able to publish the standard against which products can be tested in the future. Having good products and being able to recommend good products, the next trick is to get parents to install them and there is some great research which the children's charities have done around the number of parents who say they have installed them and switched them on and the number of products which are actually being sold and there is something of a mismatch. So the Home Secretary's Task Force, once the kite mark is in place, which should be early next year, possibly late this year, will work around accrediting products, doing more awareness for parents on what these products can do for them and how they can actually help them, and we will look at how we get products onto computers that children use at home, whether it be through pre-loading, through awareness or through other means. We are not sure what the answer is, but clearly we need to get more parents to use these.

Q76 ***Lord Sutherland of Houndwood:*** Presumably a good kite mark which was validated would provide a market opportunity which the many parents, if they were assured, would seize?
Mr Wright: The BSI kite mark is a trusted brand, which parents understand, and is an obvious choice. That is our plan.

Q77 ***Lord Young of Graffham:*** We have been talking the whole time through about security, but let us assume failure now. Let us just assume that either a bank has been accessed or even in one quite well-publicised case a laptop with all the bank details was lost. Do you think that banks or other financial institutions should be under an obligation to notify their customers that in fact there has been a breach of security, because I think there is some evidence in the past that they have not, apparently on police advice, and that does seem to me to be another creative tension?
Mr Smith: I had not heard that that was on police advice. This is an issue which we are discussing with the Office of the Information Commissioner and the

Department for Constitutional Affairs because essentially it is an extension of the scope of the Data Protection Act and the DCA lead on that. This has arisen because starting in California, but subsequently many other states in the US, they passed laws requiring companies to inform customers if their personal information had been lost.

Q78 ***Lord Young of Graffham:*** Lost or accessed?
Mr Smith: Both, accidental or deliberate loss of data, I believe, is what it covers. It is important to remember that the US does not have a Data Protection Act so they were, if you like, starting to deal with the problem from another angle. That said, I think there may be advantages in incentivising companies to protect data through that method, through actually requiring them to be named and shamed if they do not. Our instinct is to do this but to do it carefully. I think we need a study of what has happened in the US and I think there has been a lot of notifications of breaches, some of which are probably trivial and create a climate of uncertainty and doubt, which is perhaps counter-productive in the longer run, but certainly if we can use this as a tool in helping companies address security more sensibly then we would not rule it out. At the moment we have got an idea for something like this in the proposals for the communication framework review, but we doubt the sense of just applying this kind of law only to communication providers. That seems to be counter-intuitive to us, but we would not rule it out in the longer term.

Q79 ***Lord Young of Graffham:*** Yes, I appreciate the point that if every small breach was plugged the noise would swamp the message.
Mr Smith: You know what the US legal system is like!

Q80 ***Lord Howie of Troon:*** Can you tell us how many states have followed California's example?
Mr Smith: Not accurately.

Q81 ***Lord Howie of Troon:*** Is it half or—
Mr Smith: No, I think it is more than half. I think it is nearer 30 or 40.

Q82 ***Baroness Sharp of Guildford:*** Is there a big skills gap in this area of security issues, and if so what is the Government doing about it?
Mr Smith: We referred to the skills gap in our evidence essentially because we do a survey every two years of business and we are looking at what has been the impact of security breaches on those businesses and how they have responded. One of the findings of that was that there was, if you like, a knowledge or skills gap amongst businesses in how they should deal with this problem. Similarly, as we have discussed several times already, there is a skills gap by home users on the importance of keeping software up to date, for example. We tried to address both issues through outreach activities aimed at businesses. My department has a long history of providing tools and information on that subject. We have recently developed a Knowledge Transfer Network which we funded from our innovation programme to again get best practice out to businesses. I think the key way of addressing skills in the home user is the Get Safe Online campaign, which we have already alluded to several times.

Q83 ***Baroness Sharp of Guildford:*** You are not thinking in terms of any form of accreditation scheme or licensing scheme for such information on security?
Mr Smith: I thank you for the question because there is something I should have added. In the last year or so we have worked with security professionals to develop something called the Institute of Information Security Professionals, which I think is a world's first as professional body for experts in this area, and I think it is quite an exciting development. The extent to which that will lead to qualifications I think is still undecided, but it will certainly give evidence of competence and professional standing for those people, and I think that can only be beneficial. How you would actually get certification or accreditation down to the grass roots level I think is a much more difficult and long-term challenge. I am not sure I have a ready answer for you on that today.

Q84 ***Chairman:*** Thank you. I think we are going to have to wrap it up now because we are running out of time and we are losing Members of the Committee rapidly to go to the Chamber. I am going to ask a very short question and I hope there is a very short answer to it. Is the Government doing anything specific about horizon scanning?
Mr Smith: Yes.

Q85 ***Chairman:*** Via a foresight panel or something?
Mr Smith: We have had a foresight project on e-crime which looked at it over a 15 year timeframe and that is actually helping people focus on research. We have recently started a network and innovation security platform, which is a new concept, again to try and address the big social picture of how we trust networks, and within Government we have experts whose sole occupation is to look for new problems.

Chairman: Thank you very much. Your evidence has been extremely interesting and extremely useful. I do not know whether you have anything more you want to say now? We are always open to input, so if you think of something which you think might be useful to us, please write to us and let us have it. Again, let me thank you very much indeed for your very useful evidence.

Supplementary memorandum by the Home Office

Officials from the Home Office and the Department of Trade and Industry gave evidence to the Committee on 29 November, and thought it would be helpful to provide the Committee with further information which supplements the response to the question about the lack of effective legal sanctions to prevent abuse of personal data (Q 17).

In the answer it was highlighted that the Department for Constitutional Affairs (DCA) recently consulted on the Information Commissioner's recommendation that the penalties for a breach of section 55 of the Data Protection Act (DPA) be increased to a maximum penalty of two years imprisonment and/or a fine. However the timetable for the consultation process was unknown.

The Government is very keen to tackle the misuse of personal data where it occurs, which is why the DCA's consultation on an increase in the section 55 DPA penalties seeks to establish whether this was the right way forward. The consultation closed on 30 October 2006 and responses are now being considered. A summary of responses will be published on the DCA website in the coming months.

It may also be helpful for the Committee to note that the proposals would increase the penalties available to the Courts to enable those guilty of offences under section 55 of the DPA to be imprisoned for up to two years on indictment and up to six months on summary conviction (the current penalties on summary conviction are a fine not exceeding the statutory maximum £5,000, and on indictment, an unlimited fine). This would address those who profit from the illegal trade in personal information or who deliberately give out personal data to those who have no right to see it. The proposed changes reflect how seriously the Government wishes to treat those who abuse trust placed in them by their employers, or those who cajole information from organisations for personal gain.

11 December 2006

WEDNESDAY 13 DECEMBER 2006

Present	Broers, L (Chairman)	Mitchell, L
	Erroll, E	O'Neill of Clackmannan, L
	Harris of Haringey, L	Paul, L
	Hilton of Eggardon, B	Young of Graffham, L
	Howie of Troon, L	

Memorandum by APACS

APACS welcomes this opportunity to provide evidence to the Science and Technology Committee on the subject of personal Internet security. APACS is the UK trade association for payments and for those institutions that deliver payment services to customers. It provides the forum for its members to come together on non-competitive issues relating to the payments industry. We currently have 31 members whose payment traffic volumes account for approximately 97 per cent of the total UK payments market.

APACS co-ordinates a range of banking industry activities aimed at tackling payment-related fraud. One of the most visible recent initiatives has been the introduction of Chip and PIN. APACS also co-ordinates the banking industry's efforts to combat online banking, payment and identity fraud. APACS and its members have many years of experience in gaining an understanding of the threats faced by individuals using online services, and in developing effective strategies to mitigate those threats.

Summary

The level of threat to personal security on the Internet is increasing. It is driven by a combination of factors, each of which is contributing to a rapidly escalating problem which, if not effectively tackled, threatens long-term damage to the increasingly important online economy. These factors include, but are not limited to:

- the increasing sophistication of social engineering and technical threats which are mostly aimed at private individuals;
- the commoditisation of these skills and technologies;
- the increasing involvement of cross-border organised crime gangs in operating fraud and money laundering operations, and in funding the development of skills and technologies used to attack individuals;
- the challenge of providing effective information and advice to the most vulnerable; and
- the challenge of mounting an effective cross-border law enforcement response.

Our response describes the range and severity of threats to personal online security, and suggests a number of areas where the banking industry feels that valuable improvements could be made.

Defining the Problem

The nature of the threat to private individuals

Online banking and payments are hugely popular activities in the UK. APACS research estimates that nearly 16 million people use online banking services in the UK, and nearly 27 million now shop online. The Internet has therefore rapidly become an extremely important and attractive channel for payments and access to sensitive financial information. These are services that consumers value highly, and financial institutions are keen to meet this demand in a secure manner.

The security of internet-based services is paramount to the banking industry, and banks have invested heavily in protecting their IT infrastructure. These measures have been highly successful in protecting banks' customer data from direct attack. However the very strength of protection around banking systems has led criminals to target the weak link in the chain—the customers themselves.

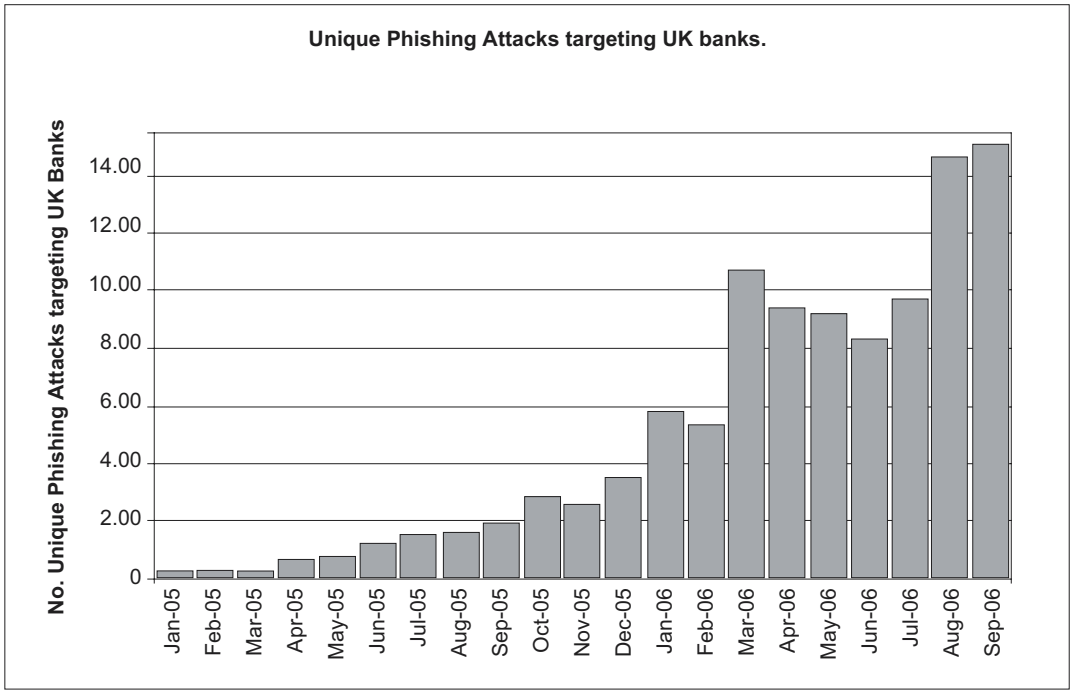
Criminals have also seen the success of the Internet, and have begun to exploit its weaknesses for their own ends. They are interested in obtaining security credentials and other information that enables them to obtain value. Such information includes usernames, passwords, card numbers, addresses, telephone numbers and

memorable data such as mothers' maiden names. Criminals generally try to steal these credentials in one of two ways:

— By asking for it: Phishing emails are a very visible example of so-called "social engineering". They are unsolicited—sent out at random by criminals, usually hundreds of thousands or millions at a time—that often pretend to be from a recognised financial institution. The emails ask the recipient to click on a link that takes them to a web site that may look identical to a genuine bank site, but whose sole purpose is to fool visitors into handing over their security credentials. Having obtained the information, criminals are then able to impersonate a customer and log into their bank account to withdraw funds, or use the information to carry out other types of identity theft.

APACS has monitored the growth of phishing since it first hit the UK banking industry in September 2003. The sophistication of the emails has evolved considerably over time, including the emergence of personalised phishing, where name and address details of the recipient are included in the email. Attackers typically obtain these personal details through identity theft, for example by stealing online merchants' customer databases. To date we have not seen any evidence to suggest that bank customer databases have been compromised, and apart from the personal details they contain, such phishing emails are still essentially sent out at random.

APACS has also monitored the rapid growth in phishing incidents (measured as the number of spoof bank sites set up by criminals—not by spam run volume) aimed at UK banks over the past few years. In January 2005 we recorded 18 such incidents, compared to 1,513 in September 2006—an increase of over 8,000 per cent in less than two years.



Phishing is not the only form of social engineering used to steal personal information.APACS expects telephone-based scams to expand, driven by the rapid takeup of Voice-over-IP (VOIP) services that allow fraudsters cheap and largely anonymous access to any UK phone number. APACS has monitored a number of cases of so-called "Vishing" over the past few months.

— By spying on the consumer: There is strong evidence that criminal gangs involved in phishing scams are increasingly using highly sophisticated software to steal data, commonly referred to as trojans, malicious software or "malware". Organised gangs have created underground markets to obtain information from corrupt researchers on computer security holes, which their own software coders can then turn into effective malware. The objective of malware is the same as phishing—to obtain personal and security information. The difference is that the victim may remain completely unaware that anything is wrong until a fraud has occurred. Modern malware is capable of infecting even well protected computers, and of spying on user activities such as keypresses, mouse movements and Internet browser sessions.

By way of example, Torpig/Haxdoor is a particularly sophisticated example of malware that is being investigated by the banking industry. Once infected by Torpig, a victim's computer waits for the victim to navigate to any one of several hundred bank web sites before inserting false login pages which invite customers to input a wide range of information. Torpig is capable of being updated automatically, and thousands of victim machines may be managed by a single criminal.

Scale of the threat

It is important to appreciate that online identity theft scams are largely run by organised crime gangs, most of them operating on a trans-national basis. Through collaboration with law enforcement, we have been able to establish that most attacks targeting banking customers emanate from a number of gangs operated out of eastern Europe, although other organised gangs are increasingly becoming involved including ones based in Nigeria.

Losses to the banking industry due to online banking fraud grew 90 per cent in 2005 to £23.2 million. Losses for 2006 are expected to increase by a similar percentage. All banks currently choose to refund customers whose accounts have been compromised, except in exceptional circumstances such as first-party fraud.

The introduction of Chip & PIN to credit and debit cards, and the high level of security that it offers, has led to fraudsters migrating their card fraud efforts to channels where Chip & PIN protection is not available—in other words to Internet and phone transactions. In 2005 card-not-present fraud rose 21 per cent to £183.2 million (of which an estimated £117.1 million was Internet-based), and there is evidence that organised fraudsters are actively seeking to obtain card details online, using many of the same techniques aimed at online banking users.

APACS estimates that the wider cost of identity theft against bank customers was around £30.5 million in 2005. This is made up of a combination of misuse of card data, fraudulent applications for accounts or funds and account takeover. Not all of the total is attributed to online activity, but industry intelligence suggests that the Internet is an increasingly popular channel for fraudsters to use both for compromising victims and for carrying out fraud.

The harm done to the UK as a result of this activity is significant. Direct losses tend to be transferred quickly abroad using a variety of money laundering techniques, where the assessment of a number of law enforcement agencies strongly suggests that much of the cash finds its way into the hands of organised criminals who use the money to fund further activities including drug and people smuggling, prostitution and terrorism.

Consumers' understanding of the threat

The often complex nature of the attacks being directed at consumers, coupled with a general unfamiliarity with the equally complex nature of computing and the Internet, means that many consumers are highly vulnerable. There is a misplaced belief that personal computers are consumer products in the same was as televisions or cameras. The truth is that although major strides have been made in hiding the majority of a computer's complexity from consumers, that complexity in fact still remains and can be taken advantage of by knowledgeable attackers.

APACS research reveals that a small but significant segment of the population remains vulnerable to social engineering attacks like phishing. In August 2006 some 4 per cent of respondents stated that they would respond to a phishing email, virtually unchanged from a 2004 survey. Younger people appear disproportionately vulnerable, with around 12 per cent of 18–24 year-olds stating that they would respond in both surveys. Although the vast majority of people recognise social engineering lures for what they are, additional research undertaken by Indiana University[1] indicates that, where phishing emails are highly personalised with accurate information about the recipient (eg name, address and other personal information) then response rates can climb dramatically. The banking industry and law enforcement agencies have seen that criminal gangs are putting more effort into obtaining and using such details to improve the credibility of their lures.

One encouraging trend that we have noted is that computer users are increasingly aware of, and are making use of, security technologies such as regularly updated anti-virus software, firewalls and operating system patches. Taken together, such measures greatly help to protect a computer against infection. However, the picture is

[1] http://www.indiana.edu/~phishing/social-network-experiment/phishing-preprint.pdf. Jagatic, Johnson, Jakobsson, and Menczer (School of Informatics Indiana University, Bloomington).

not all good. We note that the UK remains very high on an international league table[2] for "zombie computers"—computers that have been infected with malware for purposes such as identity theft, phishing and spamming. At one point last year it was estimated that nearly a third of the world's "zombie" computers were located in the UK. Often consumers express concerns about the additional costs of securing their computers, particularly with regard to anti-virus software although many free packages are available. Using security measures is increasingly essential, and users should be encouraged to think about them in much the same way that locks and alarms are now considered to be perfectly reasonable measures to have on cars and homes.

Malware writers are using ever more sophisticated techniques, including so-called "rootkit" technologies. Rootkits enable malware to—amongst other things—hide from computer users and from security software. The problem of rootkits is rated as being so severe that a senior Microsoft security manager has been quoted that often the only solution for dealing with a computer infected with a rootkit may be to "nuke it from orbit"[3] by completely wiping the hard drive and reloading the operating system and software from scratch. To expect the average computer user to detect and respond properly to such devastating attacks presents a considerable challenge.

Tackling the Problem

Information security support to private individuals

A number of UK banks offer their customers subsidised or free security software. Banks also provide customers with advice on how to protect themselves on their sites both directly and via collective initiatives such as www.getsafeonline.org, www.identitytheft.org.uk and www.banksafeonline.org.uk.

An important central consideration is that criminals are targeting consumers because consumers are able to give away their credentials to the criminal, either by stealth or by way of a confidence trick. One way of mitigating this problem would be to provide consumers with a security system in which they themselves would not form the weakest link.

Many banks are seeking to do this via the introduction of so-called "strong authentication" systems. These can take many forms and include the use of a piece of equipment (commonly known as a "token") to generate a unique passcode that could only be used once, and which would change every time it was required. In this way, a criminal would not be able to re-use any captured information. In all cases banks complement their specific customer authentication controls with additional risk management and fraud detection controls within their on-line banking service. These controls, which form a layered security approach, are sometimes visible to the customer and sometimes operate in the background, and are harder for criminals to overcome. These measures are broadly consistent with the recommendations made to US banks by the Federal Financial Institutions Examination Council in 2005.

Increasing awareness and improving education

Based on the evidence gathered by APACS, whilst the majority of computer users are generally aware of computer security threats and do take sensible steps to reduce their exposure, a minority continues to remain vulnerable. As stated previously, this is despite many high-profile media stories and educational efforts over the past few years, and indicates that future awareness-raising efforts will need to focus particularly on that group of users who remain most at risk.

These trends are despite numerous high profile initiatives put in place over the past couple of years by the banking industry, government and others to inform and educate members of the public of the threats and to provide advice on how to protect themselves. We believe that much more needs to be done in order to bring about a significant shift in cultural perceptions, and that this will require concerted and joined-up action from government, in the form of public information efforts and improvements to training and education in areas such as life skills and computer skills.

A number of factors can prevent private individuals from following appropriate security practices, including:

— Lack of computer literacy skills.

[2] Symantec Internet Global Threat Report, January–June 2005.

[3] Mike Danseglio, Microsoft Security Group Programme Manager, April 2006.

— Prevalence of inappropriate risk judgements borne out of arrogance or naivety, eg "it can't happen to me" or "I'm too clever to be taken in by such things" or even "This email must be from my bank because it's got their logo on it".

— Complexity of applying technical countermeasures, and of configuring them correctly.

— Price of countermeasures.

Stakeholders' roles in ensuring effective protection

Effectively protecting individuals online is a complex task that requires action from a wide range of stakeholders, all of whom have roles to play:

— Operating system vendors: The security and stability of the computer's operating system is the foundation upon which effective protection for all Internet based activity must be built. Fortunately there has been significant improvement in this area over recent years with the introduction of more secure operating systems which are less open to abuse, and where necessary easier to patch. It is a fundamental requirement that all operating system vendors continue to maintain this effort, and make them ever more stable requiring ever fewer critical patches to maintain their security.

— Internet browser vendors: The Internet browser is the primary way in which consumers interact with internet services, and therefore there is a need to ensure that browsers are fundamentally more secure and less open to abuse. A key improvement from a consumer perspective would be to examine how information warnings and messages are presented to the users to ensure that they are obvious and unambiguous. Far too many current messages are susceptible to being ignored or misunderstood by users and this allows them to be deceived into accepting malware that would infect their PCs.

— Computer security vendors: This includes the wide range of anti-virus software, antispyware software and firewall vendors. Here we feel that more can be done to focus more on the specific threat of malware that has been specifically written with the objective of ID theft. Often such malware is targeted at relatively small numbers of victims, and the fear is that many security vendors may not appropriately prioritise these risks.

— Internet Service Providers: The ISP community provides users with the primary means to personal access to the Internet. As such they are vital stakeholders to engage with. There is a view that more can be accomplished by ISPs in this area, which we will set out later in this submission.

— Law Enforcement: The likelihood is that the global nature of cyber-criminality will limit the ability of Law Enforcement to secure prosecutions. It is with this in mind that the concept of reducing harm to consumers is vital to promote, and law enforcement under the banner of crime prevention has a key role to play.

— Government: The Government has a wide range of responsibilities to protect consumers, most notably through the creation of effective laws and regulation that will help to prevent offences. As important, however, is providing the means to ensure that individuals are less vulnerable to attack through sound and effective education and awareness, recognising that this will be a long term enduring problem. An additional aspect of this is the dissemination of coherent and effective advice and warnings to consumers of new vulnerabilities. Here the Government could go much further than it has currently and emulate the better practice found in other nations through the establishment of a national Computer Emergency Response Team (CERT) that could exercise this function.

— E-commerce community: All those who provide e-commerce services to users should work to educate their user communities, and should take stronger action to protect the information that they hold on their customers from the possibility of being obtained and misused by criminals.

— Banking industry: In addition to their status as part of the wider e-commerce community, banks are well placed to drive forward stronger authentication measures that could provide wider benefits in the longer term. Moreover there are effective benefits in sharing knowledge of the consequences of the threat to end users, as it allows the industry to shape its messages to consumers on what they can do to protect themselves. Additionally it has allowed us to build a broader consensus on why and how personal Internet users must be protected.

— Individuals: All the security systems and advice in the world are useless if individual users fail to use them. So long as criminals continue to regard individuals as a weak link in the security chain then they will continue to be targeted. The great majority of individuals do behave sensibly and securely, but the remainder should continue to be challenged to alter their behaviour if only for their own good.

UK research into Personal Internet Security

The UK Payments Industry conducts, through APACS, a number of regular surveys on how UK consumers use the Internet for e-banking and making purchases. These surveys often include more general questions in relation to personal Internet security; some of the results of one of the most recent were set out earlier in this response.

It is important to recognise that any research into user attitudes to Internet security is challenging and ripe with paradoxes that must be confronted in the design of any future research. In simple terms this is characterised by users expressing generalised and abstract fears from a perceived lack of security on the Internet, whilst at the same time willingly using it regularly to conduct their lives. We have as a consequence seen no definitive evidence or conclusive research that security fears are driving users away from Internet services.

Overall, however, UK research in this area could be best characterised as patchy; there seems, for example, to be no large-scale academic research experiments into the threat of phishing and user reaction to it of the style we have seen in US academic institutions. There is therefore much more that could be achieved in trying to co-ordinate and promulgate the results of research into Personal Internet Security across all those conducting it.

Governance and Regulation

IT governance does not have a direct impact on mitigating threats, and is not a direct influence on consumers and personal internet safety. There are, however, implied benefits in that organisations that adopt sound methods of IT governance and which have adopted the best principles of information security management are more likely to deliver systems that are robust and resistant to attack. This will ensure that where these organisations offer Internet based services, such as e-banking services offered by APACS members to consumers, there is much greater confidence that they will do so securely and provide the necessary protection for the personal information they receive from the consumer.

Information security standardisation

The UK payments industry has been at the forefront of applying the best principles of sound information security management over a number of years, and has contributed with others to ensuring that this best practice is enshrined in international standards that others can follow; ISO 17799 The Code of Practice for Information Security Management. There is increasing evidence that certification against this code of practice is increasing globally, and that it is highly relevant to enterprises offering Internet-based services. This standard and other international industry-specific standards, such as the Payment Card Industry Data Security Standard (PCI DSS), are contributing to increasing awareness of the need to implement security in order to mitigate risk. Moreover it is argued that there are business benefits in applying these standards. Demonstrating conformance to sound security management practices and ensuring that personal information is given adequate protection is now being seen as a method to promote consumer confidence, and hence win repeat business.

A range of technical information security standards being developed in the international standards bodies complements these information security management standards. This is healthy and desirable and over time these will contribute to building security technologies suitable for the consumer market and thereby enhance personal Internet security. These standards may take some time to mature into viable secure and saleable products for the consumer market because in many cases they are predicated on having a secure PC host platform with no vulnerabilities. Our evidence continues to show that this is not likely to be achieved soon. One important technology that is often quoted in the context of enhancing personal Internet security is the use of digital signature technology. On a stable and secure host PC this would have benefit, but if the digital signature was generated on a host PC for which the provenance of the security is not known it is likely to have questionable value. This is compounded in Europe by differing national interpretations on digital signature

legislation enacted as a result of the EU e-signature directive. In some countries any digital signature meeting certain criteria has a degree of the weight of evidence in its favour that would make it difficult to question its provenance, which is not the case in the UK. The important consideration here is that it is often difficult to generate common consistent legal interpretations of information security technologies, despite common international understanding and agreements.

Information security and regulation of Internet services

From the perspective of the UK Payments Industry on-line Internet based financial services are regulated under the existing regulations that govern how any other financial service is offered to UK consumers. There are distinct challenges when considering the appropriate regulatory environment for other industries as they start to offer Internet services. On the one hand the relatively low cost to offer internet services with possible rich rewards makes it an attractive business channel, whilst on the other any severe regulatory burden could markedly constrain growth. This is compounded by the lack, at least early on in the lifecycle of a service, of any prevailing threat that would dictate regulation or security. However, as we have seen in recent years the speed with which criminals have been able to exploit a wide variety of disparate channels for their profit is alarming.

An example of lighter touch regulation, which at the time was appropriate and relevant but perhaps now needs to be re-examined, is Section 17 of the Electronic Commerce (EC Directive) Regulations 2002. This section, known as "Mere Conduit", ensures that ISPs are not liable for any information that passes over their networks. Whilst this is entirely reasonable it has been used as defence by the ISPs for why they will not monitor, and then take action against, their customers' host PCs that have been compromised and are then used by criminals to send spam, distribute malware or otherwise act maliciously.

There are other countries, such as Australia, where there is much greater debate on this issue. In these cases the argument is now being made in favour of ISPs being seen to operate responsibly and to actively monitor their networks for customers' PCs that have been compromised and then advising them on remedial action. Given the fact that UK has been recorded[4] as having one of the highest rates of compromised PCs in the world, it is possible to argue that a similar policy in UK would substantially improve personal Internet safety.

Crime Prevention

The UK Government made a major step forward a number of years ago in establishing the National High-Tech Crime Unit (NHTCU) and in resourcing regional police forces' computer crime units which provided the framework for national policing of cyber crimes. APACS was a net contributor to the development of the NHTCU and maintained a very close relationship with the unit throughout its operational life. This provided an important foundation for the joint activity in responding to, and combating since September 2006 the rise in attacks against e-banking customers in UK.

Domestic dimension

It was, therefore, with considerable interest that we have tracked the merging of the NHTCU within SOCA as the e-Crime directorate. It is commendable that in this process more resources were to be given to the unit, and at the same time a realignment of responsibilities saw the remit for child pornography passed to the Child Exploitation and Online Protection (CEOP) Centre. Both of these factors should enhance SOCA's ability to address the broader issue of cyber crime of which prevention is a major element of their strategy.

The dilemma is that in subsuming NHTCU within SOCA their primary remits as a national centre of excellence upon which regional forces could draw as required, and as the guardians of the discipline of investigating cyber crime can no longer be applied. As such there is a gulf in this area within the UK that is reducing the effectiveness of cyber crime prevention. The recent proposals by Commander Sue Wilkinson of the Metropolitan Police, who is the ACPO lead for this topic, for a national co-ordinating body on cyber crimes is one that APACS warmly supports.

[4] http://news.bbc.co.uk/1/hi/technology/4369891.stm

13 December 2006

International dimension

These attacks against e-banking, and other cyber attacks such as the denial of service attacks against on-line gambling sites, are a global problem from criminals who themselves operate globally. NHTCU, and now SOCA, led the initiative that has seen marked progress in establishing the necessary framework of international co-operation amongst law enforcement agencies needed to combat these threats. We have fully supported this effort and where necessary complemented it by establishing our own peer relationships with similar communities of interests affected by e-banking attacks in other countries, most notably Australia, Brazil, Germany and the USA. The UK continues to be one of the most effective in establishing this form of international co-operation.

Computer crime criminal law

One of our major points to the All Party Internet Group on their review of the Computer Misuse Act was the proposal to make the penalties greater and to include DoS attacks explicitly within the scope of the act. The recent proposed improvements to the Computer Misuse Act included in the Police and Justice Act, are very positive indications of the Government's willingness to continue to improve existing legislation. A further example is the Fraud Bill, which will provide powers to combat deception as a means of executing fraud; this will therefore make phishing illegal and is welcomed by the industry.

As important as these moves are, there is a need for legislation that is clear and that will provide a measure of stability as technology changes. In this light the industry was concerned about some of the proposed changes to the CMA under the Police and Justice Act that criminalise security tools, although reassurances have been given that the intent is not to prevent enterprises using these tools to ensure the security of their own systems. The important consideration, however, is that any legislation designed to combat cybercrime needs to be carefully framed if it is not to have unwarranted consequences for legitimate activity that promotes security.

11 October 2006

Memorandum by Visa Europe

Executive Summary

Visa Europe is a payment solutions company owned and controlled by over 4,500 European member banks. The company's role is to provide products and services that make transactions fast, secure and convenient.

Visa secures the payment system by building multiple layers of protection around each component of the transaction chain. We are constantly striving to improve security. As a result, the overall fraud rate (fraud to sales by cards issued) is at an all time low of just 0.051 per cent. Due to the introduction of Chip and PIN, counterfeit fraud has been reduced. The fastest growing type of fraud, however, is "card not present", which now accounts for 40 per cent of cases. Visa has introduced a number of tools to help cut this type of fraud. These include Verified by Visa, which make online transactions more secure; CVV2, which make mail order and telephone order transactions more secure; Address Verification Service, which allows for the authentication of cardholder details; an Electronic Commerce Indicator, which validates e-commerce transactions.

Visa Europe is currently piloting Dynamic Passcode Authentication, which will make a further contribution to a safer online environment. VISOR (Visa Intelligent Scoring of Risk) is Visa's fraud detection system which uses neural networking technology to assess the validity of individual transactions. Account Information Security is designed to protect sensitive account and transaction data in the retail environment. It is currently being adopted across Europe. A variety of other technologies are explained in the attached paper.

Visa Europe has a dedicated resource that is responsible for investigating the phishing emails and contacting the host to get such sites shut down. In April 2006, Visa signed an agreement with the Child Exploitation and Online Protection Centre (CEOP). CEOP provides a single point of contact for the public, law enforcers and the communications industry, enabling suspicious activity to be reported direct, 24-hours a day. CEOP also offers advice to parents and potential victims.

Visa is committed to increasing and developing new forms of internet security. It understands the seriousness of the issue and the wide ranging damage that can be caused, not just financially, but to confidence in the whole economic system.

About Visa Europe

Visa Europe is a leading payment solutions company owned and controlled by over 4,500 European member banks. Through our brand, services, systems and operating regulations, we enable our member banks to meet the needs of their customers and merchants but also to take part in the global Visa system.

Our role is to provide products and services that make transactions fast, secure and convenient. To achieve this, we connect the different parties in the payment process.

Through Visa:

- Issuing banks provide consumers with a universal payment method.
- Consumers benefit from convenience and security.
- Retailers benefit from speed, lower cash handling costs and security and provide their customers with a popular payment service.
- Acquiring banks provide retailers and merchants a popular, universal way to accept payments.

Visa has recently announced plans to globally restructure its organisation. Its businesses in the USA, Canada, Asia Pacific, Latin America and Caribbean, Central and Eastern Europe, Middle East and Africa (CEMEA) will be merged to become a publicly-traded company, Visa Inc. In Europe, Visa Europe will remain as an independent membership association, owned and governed by its 4,500 European member banks.

The decision to retain Visa Europe's membership-owned, not-for-profit association structure, will enable it to directly support the development of the European internal market in payments and the Single Euro Payments Area (SEPA). At the same time, Visa Europe will receive an exclusive licence from Visa Inc, ensuring global inter-operability.

Fraud—General

There are many parties involved in a Visa transaction—a cardholder, a merchant, often a processor, and issuing and acquiring banks. Visa secures the global payment system by building multiple layers of protection around each component of the transaction chain. Occasionally criminals may exploit one component of the payment system, but our multiple layers of protection respond quickly and minimise impact to cardholders. Sophisticated neural networks rapidly identify suspicious activity and allow banks to take action.

From the moment we plan an activity, we do all we can to minimise risk and maximise confidence though our security initiatives. Our approach is to anticipate, analyse and address issues, provide guidance and clear communication, while fostering co-operation.

To remain one step ahead of criminals, Visa continuously enhances security by improving technologies, leading cross-industry collaborations and working with law enforcement authorities. Visa also supports consumer education and awareness programmes. Many of these advances are targeted at protecting online purchases and securing data in the digital world. Visa aims to prevent fraud, and when it does occur, to minimise the impact. As a result of our efforts, the overall Visa Europe fraud rate (fraud to sales by cards issued) is at an all-time low of just 0.051 per cent. Due to the introduction of chip and PIN in the UK, counterfeit fraud has been reduced. The fastest growing fraud type is now "card not present" (CNP) which accounts for 40 per cent of fraud. Visa has a wide armoury of tools to combat CNP fraud (fraud in the telephone, mail order/telephone order (MOTO) and internet environment).

Verified by Visa (VbV)—Making Online Transactions More Secure

Verified by Visa is an authentication system based on cross-industry standards. A free service to the cardholder, Verified by Visa provides proof that a genuine cardholder and a genuine Visa retailer are taking part in an online transaction.

Cardholders who enrol for the scheme choose their own password. When they make a purchase at participating Verified by Visa e-tailers, they are prompted for the password to prove they are who they say they are.

In the UK, there are currently over 12,000 retailers signed up to Verified by Visa, including NEXT, Dixons, Dabs, British Airways, John Lewis, Opodo and Tesco, and numbers are growing fast. In the UK, there are more than three million cardholders enrolled in Verified by Visa and this number is increasing by 90,000 to 120,000 per month. Approximately one in eight online UK Visa transactions are Verified by Visa transactions.

CVV2—Making Mail Order/Telephone Order (MOTO) Transactions More Secure

Particularly for telephone orders and online shopping, one of the most effective yet simple security measures is the three-figure CVV2 number—a "static" authentication code—printed on the reverse of the card on the signature stripe. Merchants request the number as evidence that the shopper has possession of the card when making a purchase. CVV2 numbers have been incorporated on all UK cards for some years.

Address Verification Service (AVS)—Authenticating Cardholder Details

AVS provides another level of security, by authenticating the billing address on the card. In the event the card has been stolen or cloned, corresponding billing address info will not be available. If the billing address details are incorrect or not known, this is flagged to the issuing bank which can decline authorisation.

Electronic Commerce Indicator (ECI)—Validating E-commerce Transactions

ECI indicates e-commerce transactions and identifies the merchant type, ie: flowers, hotel, etc. This allows banks to identify such transactions and make informed authorisation decisions. E-commerce transactions which pass through the Visa system are grouped and reported to Visa member banks.

Dynamic Passcode Authentication—Creating a Safer Online Environment

Another advance—known as "dynamic passcode authentication"—is being piloted by Visa Europe. Dynamic passcode authentication brings the added security of chip and PIN to online transactions and is being gradually rolled-out by Member banks for e-commerce transactions at VbV merchants. We are currently exploring how dynamic passcode authentication can work for telephone order transactions (using VbV) and pilots are being planned in a few major markets within Europe.

Devices (known as "Form Factor") to enable dynamic passcode authentication can vary but generally the cardholders would be given a pocket-sized reader. Each time the cardholder makes a purchase at a Verified by Visa e-tailer, they insert their card into the handheld reader. They then type into the reader's keypad their PIN code—validating they are in possession of their card—and prompting the reader to generate a one-time "dynamic" passcode based on chip and PIN cryptographic algorithms. When the cardholder comes to pay at the website's checkout page, they type in their card number and this will generate a request for the dynamic passcode. For added security the cardholder may be given a "challenge" that would also be entered into the reader and together with the PIN, a "response" would be generated by the reader that would be sent securely to the Member bank for verification.

The dynamic passcode authentication is therefore based on "two factor" authentication ie testing that the card is in the cardholder's possession and that the individual knows the corresponding PIN code. The one-time passcode is useless for subsequent transactions and the reader is always offline and therefore not at the mercy of hackers.

In addition to measures targeted specifically at protecting CNP transactions, Visa has other security measures, which protect banks, retailers and cardholders from fraud in all purchasing situations. These include:

Visa Intelligent Scoring of Risk (VISOR)—Visa's Fraud Detection Solution

VISOR is a Visa Europe fraud detection solution that employs neural networking technology, which mimics the processes of the human mind to assess the likely validity of individual transactions. Every transaction that passes through VisaNet is closely scrutinised by VISOR. VISOR uses a number of components to provide a highly accurate score you can rely on.

Components include:

- Visa Europe Model—trained and refreshed once a year with both current fraudulent and genuine spending patterns.
- Cardholder profiles.
- Merchant profiles.
- Sophisticated fraud detection rules.

Each time a transaction passes through VisaNet it is automatically routed to the VISOR neural network for analysis and scoring. The transaction will pass through the Visa Europe model, cardholder and merchant profiles and will generate a score based on the interactions between the profiles and the model. The higher the score, the higher the probability of fraud. The issuing bank can then decide whether to authorise or decline the transaction.

In addition to providing accurate risk scores, VISOR also acts on sophisticated fraud detection rules to target particular types of high-risk transactions. Rules are specifically useful when combating emerging fraud trends or "flash frauds" that would otherwise not be detected by the neural network. Rules can be global, country or Member specific.

Account Information Security (AIS) Programme

The AIS programme is designed to protect sensitive account and transaction data in the acceptance environment, when it is used and stored at merchants and third-party service providers. The programme protects the interests of all participants—banks, merchants and cardholders.

Visa was the first in the industry to create such a programme, including standards, best practices and self-assessment security tools. AIS is now a cross-industry standard (known as PCI DSS—payment card industry data security standard). In order to qualify as "AIS compliant", individual banks, merchants and service providers have to prove that they meet standards controlling their data handling and storage procedures. AIS is currently being adopted across Europe.

Other Programs and Initiatives

Visa Europe systems constantly monitor transactions, detecting patterns which require investigation, checking identities and validating payments. We know where risks are prevalent and where vulnerable points need to be observed or addressed.

Visa Merchant Alert Service (VMAS)

The Visa Merchant Alert Service combines monitoring programmes for issuers and acquirers alike, identifying disproportionate losses, especially in cross-border transactions.

The service allows acquirers to assess a merchant's past record before signing them up. At every opportunity we help connect a network of anti-fraud organisations through the regular publication and sharing of relevant data. A database of terminated merchants is also made available.

Risk Identification Service (RIS)

The objective of RIS is to help Acquirers reduce fraud by identifying merchant locations where risk-related activity is taking place. The RIS system gathers and analyses transaction and fraud data from a variety of sources and compares risk-related activity occurring at merchant locations against a set of parameters (also known as Visa standards). If risk activity at a merchant exceeds any of the parameters, RIS produces an identification report that is sent to the Acquirer for investigation. Depending on the severity of the identification, ie which parameter has been exceeded and by how much, Visa may require additional action to be taken to control the fraud.

Visa Account Bulletin (VAB)

The Visa Account Bulletin is an online tool used to alert member banks to specific account numbers that may be at risk or of immediate concern. In the event of accounts being compromised the Visa Account Bulletin is a rapid and secure distribution tool that provides account numbers to each specific member.

The application focuses on distribution to Issuers, and uses the Issuer BIN (first six digits on the card), extracted from the account number in order to contact the Issuer. The Issuers are contacted via email and the account number details are stored on VOL (Visa Online, a dedicated Visa extranet application). Once the Issuer has received an email alert, they should log onto the system and download account numbers, and details of the alert.

Alerts are sent to some or all issuing banks, depending on the situation, drawing their attention to issues and actions required to contain the problem. There is also a news section, which summarises recent developments, as well as a link through to the Global Fraud Information Service (GFIS).

Global Fraud Information Service (GFIS)

The GFIService is an online resource, providing timely information and tools to the wider fraud-fighting community—ie beyond the immediate Visa network.

GFIS publicises trends, issues alerts, provides information about investigations, and lists contacts (within Visa, its members and law enforcement bodies). GFIS also publicises products, programmes, relevant courses and best practice guides.

With a useful search facility, it enables Visa, its members and global contacts to stay updated and equipped in the battle against fraud, both regionally and worldwide. GFIS also provides benchmarking data to enable banks to compare performance against their competitors.

Anti- Phishing Measures

Criminals have developed effective and sophisticated methods to collect personal information from unsuspecting cardholders by using emails and also "spoofing" legitimate Internet websites. Unsuspecting cardholders are caught in these schemes where their Visa account information or personal information is captured and then used to commit fraud. Visa Europe has a dedicated resource that is responsible for investigating the phishing emails and contacting the host to get sites shut down. Visa actively informs its members by placing alerts on the GFIS to inform and communicate these phishing instances.

Training and Education

A vital aspect of Visa's work is training and educating members and law enforcement agencies. By providing a range of courses and best practice guides we help members to gain a better understanding of the issues relating to CNP fraud and how to combat the problem using some of the risk management tools. Also, we maximise every opportunity to provide advice to cardholders on this matter through our PR activities and via our website.

A course we have recently developed is focused on the Internet and Phishing. It is aimed at fraud investigators at member banks to inform them of the tools and methods available for tracing and combating Internet fraud and phishing.

When shopping online, many of the simplest and most effective preventative measures are in the hands of cardholders. Visa advises customers:

- If suspicious, check an e-tailer's security credentials or call its customer helpline for reassurance.
- Only use a computer that has appropriate levels of up-to-date security eg anti-virus software and a firewall.
- Keep passwords private and change them often. Create passwords that would be difficult to guess, preferably a mix of letters and numbers.
- Keep transaction records, just as you would save your receipt in a shop, including the merchant's contact details and internet address.
- Beware of unauthorised e-mails or sites requesting information such as PINs, do not divulge information unless given explicit instructions by your bank. Do not accept instructions via e-mail, as these may be fraudulent.
- When asked to provide payment details, ensure you are at the correct site. Check for presence of the "padlock" security symbol in the browser window and click on the padlock to reveal information regarding the owner of the website security certificate.

CEOP—The Child Exploitation and Online Protection Centre

Visa cards and products are not to be used for any unlawful purposes. While laws governing child pornography may vary from country to country, we are unequivocal about our position on this activity. Very simply, we do not allow Visa products to be used to facilitate these transactions.

Visa will work with its members to ensure that acceptance privileges are terminated for any merchant dealing in child abuse images anywhere in the world, irrespective of local laws or customs.

Visa will continue to support a programme to combat, and if possible, prevent its products being used for the acquisition of such material.

In April 2006, Visa signed a three-year partnership agreement with the newly created Child Exploitation and Online Protection Centre (CEOP). CEOP provides a single point of contact for the public, law enforcers and the communications industry, enabling suspicious activity to be reported direct, 24-hours a day. The unit, staffed by about 100 police, computer technicians and child welfare specialists, also offers advice to parents and potential victims.

Visa will provide financial support and all its knowledge and resources to strengthen CEOP's finance desk, which identifies people engaged in the sexual exploitation of children for profit and sets out to confiscate offender's assets and disrupt their activities.

Conclusion

Visa is committed to increasing and developing new forms of internet security. It understands the seriousness of the issue and the wide ranging damage that can be caused, not just financially, but to confidence in the whole economic system.

Visa believes that Government could do more to promote new anti-fraud measures by using them within its own services to citizens. For instance by asking HM Customs and Revenue and HMSO to use Verified by Visa, many more people could be encouraged to sign up to the service. This would make the whole payments environment more secure.

Whilst Visa realises that the Government alone cannot deal with the whole issue of personal Internet security, we believe that more can be done to get consumers to take responsibility for keeping their financial information secure. Government departments are well placed to do this and Visa would be happy to support any government initiative highlighting the seriousness of this issue to the public.

October 2006

Examination of Witnesses

Witnesses: Mr Colin Whittaker, Head of Security, APACS, Ms Sandra Quinn, Director of Communications, APACS; Mr Matthew Pemble, Chairman, Joint Special Interest Group, Federation of Incident Response and Security Teams and the G8 Line Group; Ms Sandra Alzetta, Senior Vice President for Consumer Market Development, Visa, and Mr Robert Littas, Senior Vice President Fraud Management, Visa, examined.

Q86 ***Chairman:*** Welcome, everybody. This is the second evidence session of the Select Committee's inquiry into Personal Internet Security. We are very grateful to all of the witnesses who are coming to give evidence today. Thank you very much for coming along and giving us your time. Welcome, also, to the members of the public who are here. There is a document available—I hope you have picked it up—about the inquiry and the Members of the Committee. To start with, could you introduce yourselves and, if you so wish, make a brief opening statement. So perhaps we could start with you, Ms Quinn.

Ms Quinn: Good afternoon. My name is Sandra Quinn, I am Director of Communications at APACS. APACS represents the banks in how to co-ordinate their fight against payment fraud.

Mr Whittaker: My name is Colin Whittaker, I am Head of Security at APACS.

Mr Pemble: My name is Matthew Pemble. I am appearing as the Chairman of the Joint Special Interest Group between the Federation of Incident Response and Security Teams and the G8 Line Group in co-operation between computer emergency response teams and law enforcement, and as co-chair

of the Best Practice Committee of the Anti-Phishing Working Group.
Ms Alzetta: My name is Sandra Alzetta, I am the Senior Vice President of Visa Europe responsible for consumer marketing and my responsibility is for the eCommerce channel, the Internet channel, from a business perspective.
Mr Littas: I am Robert Littas, Head of Fraud Management in Visa Europe.

Q87 ***Chairman:*** Would any of you like to make an opening statement or shall we go straight into questions?
Ms Quinn: Please go straight in.

Q88 ***Chairman:*** Okay, we will go straight into questions. I will ask the first question. In 2005 online banking fraud increased by 90 per cent to £23.2 million. Do you have any indications as to whether this rate of increase will be sustained in 2006?
Ms Quinn: If I may answer that. Those figures are APACS figures which we put together with our member banks. It was £23.2 million at the end of 2005. We have half year figures for the first half of 2006, and those stood at . . .
Mr Whittaker: Those were the £23.21 million. It was £14.5 million in the first half of 2005.
Ms Quinn: For the first half of 2006 the online banking fraud figure stood at £22.5 million. That was an increase of 55 per cent in the first half of 2006 on 2005. Obviously we are not at the end of 2006 yet so we do not have the full year's figures but we expect the overall rise in this year not to be as high in percentage terms as the rise in 2005.

Q89 ***Chairman:*** But it looks as if it might be close to, you are saying?
Ms Quinn: It is certainly not going to be a non-dramatic rise, it is still of concern.

Q90 ***Chairman:*** The evidence from APACS notes that the number of phishing incidents grew by 8,000 per cent between January 2005 and September 2006. Is this phenomenal rate of growth continuing? How much are the banks now losing to phishing, and how much worse do you expect it to get?
Mr Whittaker: The rate of growth in phishing is really down to a number of factors, not least of which is they have been able to industrialise the methods by which the criminals know how to launch and sustain the attacks. Secondly, it is perhaps an indication of how well the banks have been doing at closing the sites down. The more the banks close down the people attacking us and launching the phishing sites, the more they have to launch to try and generate the attacks against us. We see no indication worldwide that the level of phishing attacks is decreasing, in fact there is some evidence that we were talking about on the way in, that the phishing incidents are increasing, again worldwide. The level of losses from phishing, the overall figures that Sandra described, include both phishing and malware based attacks. It is very difficult when you are talking to consumers to distinguish between whether they have fallen victim to a phishing or a malware attack. By and large, we believe that the sort of questions that the bank call centres are able to ask the consumers when they discuss with them the problems with a fraudulent transaction, for example, can very quickly discern whether phishing attacks have occurred because people are talked through a script about the sort of things they might have seen on their computer and the way they may have behaved when an email, for example, comes in. By and large we reckon, and it is very difficult to be totally specific about this because of the difficulties of attributing attacks, that phishing accounts for anywhere between 25 and 50 per cent of the attacks that we see that cause losses on customer accounts.
Chairman: Does anybody else want to comment on that?

Q91 ***Earl of Erroll:*** I notice you mentioned phishing attacks as the number of websites which are trying to phish.
Mr Whittaker: Yes.

Q92 ***Earl of Erroll:*** Are more people responding to these phishing attacks or fewer? In other words, is the public getting better educated about them and avoiding them regardless of the number of sites?
Mr Whittaker: It is very difficult to determine because the point of attributing these attacks when you talk to people is at best subjective. Our indications from some data that we have been able to correlate between the number of fraudulent transactions and the number of phishing attacks over the years is that it seems people are falling victim to phishing attacks less often, but that is one of the reasons why they are increasing the volume, because of the number of people they may have to capture and so on.

Q93 ***Lord O'Neill of Clackmannan:*** Are you satisfied that all of your members are equally rigorous in the way in which they seek to protect themselves from phishing? All I can say is that when I tried to open an account in one financial institution in Britain against another there seemed to be a certain number of hoops and hurdles that I had to go through with one institution but not necessarily with the other. I just get the feeling that there is an unevenness about the security considerations, some seem to be overly complicated and others might be unduly simplistic. Do you impose standards on your members?

Ms Quinn: We do not have the authority to impose standards on our members but what they all need to do is assess their own levels of risk and the levels of risk that they are able to accept in their relationship with their customer.

Q94 ***Lord O'Neill of Clackmannan:*** Do you have a name and shame process within the organisation? We know that you are very secretive as far as the general public is concerned, but as far as your members are concerned—you may not have the authority to impose something—you can surely expose the inadequacies of some of the people who bring this threat on the rest of the members.
Ms Quinn: We collect fraud figures that members report to us and each individual member will know their level of fraud as a percentage of the overall loss, so they will be able to very quickly assess themselves as to whether their fraud is a larger percentage as opposed to a lower percentage and they will know how that has happened. The other point to make is that with phishing attacks it is certain banks that are attacked in the UK more than others. Obviously fraudsters are very aware of the kind of banks that we bank with so they tend to attack the banks that are the names in the high street.

Q95 ***Lord O'Neill of Clackmannan:*** Or the ones that are easier to catch, the fat slow movers?
Ms Quinn: No.
Mr Whittaker: There is no evidence of that.

Q96 ***Lord O'Neill of Clackmannan:*** Is there no evidence because you do not try to collect it or is there just no evidence?
Mr Whittaker: There is no evidence that one bank is any worse or any better off than any others. Sandra is absolutely right, there has been a preponderance of certain banks attacked but that has changed over time. We have seen the ratio of different banks being attacked change with the decisions of the potential people who are launching those attacks. When it comes to the degree to which the industry co-operates in sharing, shall we say, best practice and good practice in the way in which they fight these things, I have been on the inside of the industry for some time now and have been very impressed with the candour and rigour with which they approach these areas and their willingness to share information about how they architect their sites, how they share information, particularly on the types of attacks, and learning from those. It is quite profound. Some of it has to be sensitively handled because we do not want to expose how well we know the type of methods of attacks they are launching with us. Sometimes those methods give us a way to be able to detect when a potential customer is falling victim although they might not realise it themselves.

Q97 ***Lord Mitchell:*** I may have missed a trick on this but I have not seen any publicity at all on phishing as such as a member of the general public. I wonder what sorts of initiatives you are taking to make people aware. I do not see advertisements, I do not see anything like that.
Ms Quinn: Perhaps I can start on that. We launched a website in October 2004 called banksafeonline.org.uk. That was about a year after these types of phishing attacks first started. That was specifically to make customers aware of the types of attacks that could happen and gave them an avenue to advise us of the types of attacks they were suffering. We get a number of individuals contacting us on a daily basis about the type of attack they have, trying to verify whether they are attacks or not. We have done a lot of work, particularly in the media, specifically to alert people to this. One of the key responsibilities is with individual banks to advise their customers and they have all done that in very active ways. Specifically, if you log on to your bank website they will all say to you, "We are aware of phishing, this is what this type of thing is" and there will be some very key core messages about "Your bank will never communicate to you in this way".

Q98 ***Lord Mitchell:*** How about the people who are less adept at using the Internet, who are doing it for the first time and they are getting this spam stuff through? It is all very well you giving me a website which, frankly, I have never heard of, and I am not naı£ve in these things, but it seems to me that there has not been much of an initiative to make the population at large aware of the problem.
Ms Quinn: What we have done is targeted those customers who use the Internet and who bank online because those are the people who are going to fall victim to this. Customers who may receive an email but do not bank online are less likely to fall prey to this type of activity. The key thing here is targeting your customer awareness where it is going to best have an effect.
Mr Whittaker: Certainly from our perspective, on the banksafeonline site which we manage and operate and provide all the content for, we monitor regularly the responses we get from consumers who are responding. The uptake and level of response certainly shows that people are reading and visiting the site quite regularly, it is one of the most well visited sites that we have in our APACS portfolio of information sites. We also get a lot of value from what the consumers report. One of the areas they can report, for example, is when they see a phishing email

they are encouraged to report it to a web link that we have where we handle that sort of information.

Q99 ***Lord O'Neill of Clackmannan:*** Have the numbers increased?
Mr Whittaker: Yes, significantly.

Q100 ***Lord O'Neill of Clackmannan:*** Can you give us some hard figures?
Mr Whittaker: If I remember rightly, in September we were approaching about 35,000 emails a month.
Ms Quinn: We had a fraud initiative at the beginning of November where we specifically went out to the population to encourage people to protect their PINs, their passwords and the personal information that we all have, and at the same time we were releasing the up-to-date fraud figures to give some level of assessment so that people could understand what the risks were. We highlighted in particular the website that we have there and the other website that we have, which is the Cardwatch website, and the number of hits that got increased by 300 per cent in that month.

Q101 ***Chairman:*** Have the banks informed people about the website?
Mr Whittaker: Yes, they do. They do on their own web pages. It is interesting that when some of the banks notice that there are what we call phishing email lines going out for their brand they put a notice on their website which links to our website and we can see and track which people are referring to our banks' websites and we can draw direct correlations between when brands are under attack and when they put a notice on the websites and hit rates from that bank or that bank's customers.

Q102 ***Earl of Erroll:*** Banks have set a great deal of store by their customers having to authenticate themselves properly on the website, and there is a lot of talk about bringing in further authentication. Forgetting about that, what about websites authenticating themselves to the customers and the users, surely would get rid of a lot of the phishing problems if people could be certain they were visiting the right website.
Mr Whittaker: I think there are a lot of initiatives coming on shortly technically that will help in the future and we will have to examine their impact. Microsoft's recent announcement of the extended validation certificates that they are issuing to certain institutions may go a long way to helping that when IE7 and Vista are jointly launched together in the future. When it comes down to it all banks rely on using the current method of authenticating sites, which is using secure web sessions and so on, and those can provide a measure of confidence that you are at the right site.

Q103 ***Earl of Erroll:*** Am I allowed to name banks? For instance, the one I was going to mention, Alliance & Leicester, I know uses a picture chosen by someone, so when someone goes on to their website when they log in as a user the website is effectively authenticating itself back to the user. I know that is not perfect but there are some simple techniques which seem to be being ignored by other banks.
Ms Alzetta: I would just like to explain Visa first of all and the silence until now from both Robert and myself. We are a membership association of banks who look after online shopping, so our responses will be very much with regard to online shopping as opposed to online banking, which is not our area. It is from an online shopping perspective that we know from the consumer's perspective there are some huge benefits to be gained from online shopping. This is very much an area that we are looking at just now. We have done a lot of work in this area and we know that there are some concerns about security. There are consumer concerns about security and there are issues with security. We are doing a number of things about this now and one of them is to do with authentication. We have introduced a new system called Verified by Visa. The idea is very similar to what is happening on the high street. On the high street the banks and the retailers have now invested in Chip and PIN. I am sure everybody here has a card, you will have a chip on the card, and when you go to buy something at a retailer you will now be asked to put in your four digit PIN number. That confirms you are who you say you are, as nobody else could know your PIN number, so you are confirming your identity, you are authenticating yourself. Until now that has not been the case online, so as a consumer I do not know who the merchant is and the merchant does not know who the consumer is. By introducing Verified by Visa, we are trying to replicate online what is happening on the high street. Participating merchants in Verified by Visa will have this logo on their site. This means as a cardholder I will go through the normal checkout procedure and when I get to the final page asking me to input my card details, I will put them in and the next thing I will see will be a page from my bank who has given me my card. The reason I will know that page has come from my bank is because there will be something on that page which will be my personal security message which I chose, so it is obviously not a phishing page because I chose that message. My cat's name is "Moochie", for example, so it could be that. I know it has come from the bank. It will ask me to put in my password, a pass code that I have chosen. I will put it in and it will go to the issuing bank who has given me

the card and they will confirm that the two match. If they match there will be a positive response back. If they do not match there will be a negative response back. That is the first step in introducing authentication online. What that does from a consumer perspective is make the consumer feel much more comfortable that it is possible to shop safely online and from a retailer's perspective it means that retailers can have much more confidence in accepting cards online.

Q104 ***Earl of Erroll:*** Do you have a high percentage of take-up from retailers and banks on this?
Ms Alzetta: We have been working on this for a couple of years and what we have learned from Chip and PIN is when you are talking about infrastructure it takes time. Just now we have around about 15 per cent penetration. We think this is going to be an important year for Verified by Visa, the reason being that quite recently some of the very large retailers have joined. British Airways has been a participant for some time. We have lastminute.com, John Lewis, Next, Tesco joined a couple of weeks ago, and in the forthcoming year we expect to see Ryanair and many other large retailers. In total we have got many thousands but what really matters is the big names who give the big volume. We are working with the banks and the retailers to introduce this.

Q105 ***Chairman:*** You describe a lot of this very well in your paper and you are also advocating that the Government should take up some of these initiatives as well.
Ms Alzetta: Yes. I think anything that encourages further security has got to be good news. The research that we carried out with our consumers told us that there is a concern amongst consumers about shopping online, the number one concern is security. There are various other things but that is still the number one concern. 30 per cent of the people we asked said security was a concern for them. The reality is that whilst it is our job collectively here to look continually at what is happening to make sure that we stay one step ahead of fraudsters, fraud is still is very small portion of what is happening in the Internet world. A lot of consumers are not shopping on-line because they still have some concerns, which is a real pity for them in that there are lots of advantages to be gained from shopping on-line.

Q106 ***Lord Harris of Haringey:*** Is there not a problem that what happens is you are now requiring individual members of the public to acquire yet another password and yet another security code, and people are now faced with such a plethora of passwords and security codes that the natural thing to do is you write them down, or you place them on your own computer somewhere where you can find them but of course anyone who might have access to that could find them. Is there not a problem that you are creating systems—and there are a whole series of different systems being replicated—which are in fact going to make it more difficult for the public who will then take simplistic measures by perhaps using the same password for absolutely everything? Are you not increasing vulnerability rather than reducing it?
Ms Alzetta: That is certainly not our intention and it is something that we are looking at for the reasons you have said. I think everybody here will be familiar with the fact that everything you want to do on-line will require some sort of password. The idea obviously is to add security, not to take it away. So first of all we would say to people the usual things, choose your password carefully and so on. The next step for Verified by Visa is to introduce what should be a more simple way for people to authenticate themselves and it is using Chip and PIN technology, and that was referred to earlier. The idea there will be that cardholders will use their standard Chip and PIN card, put it into a portable reader and they will put into this reader their PIN number, the PIN number that they use on the high street that they are very familiar with, so there is no need to remember separate pass codes. By putting in the PIN number, you are confirming that you are the valid cardholder. A unique one-off number will be generated and that is the number that you will then put into the on-line shopping site. So it does two things. It will increase the level of security because instead of having the same password each time, you are putting in a one-off number which once it has been used it cannot be used again. It is confirming that you are who you are because nobody else has your PIN number but also, most importantly as a consumer, all you have to remember is your PIN number which is the number you use every day on the high street. We will start seeing that rolled out by some of the UK banks in the summer of next year.
Chairman: This is well described in your memorandum. It would be useful for us to have data about the take-up of these ideas. I think we are going to have to move on. Lord Paul?

Q107 ***Lord Paul:*** Can you provide for us a detailed breakdown of the £23 million of fraud. What kinds of fraud are involved?
Ms Alzetta: I think that is the APACS figure for on-line banking fraud.
Mr Whittaker: As I was saying earlier on, those £23.5 million frauds (£25 million worth of losses) is down to on-line banking fraud, and it is wholly down to people making fraudulent transactions on people's accounts across a range and variety of sorts of accounts that the banks allow Internet access to.

There is no evidence yet to believe that any of the compromise of Trojan or phishing against on-line bank accounts has led to anything in the sense of identity theft in the sense of the taking of people's identities. It has been solely down to making fraudulent transactions from the victim's account to a middle account which we call a "mule" account.

Mr Pemble: There are essentially three main fraud methodologies involved in these sorts of figures: phishing, which is the one that has already been described, where you get sent essentially a spam e-mail which has a link in it to a fraudulent bank site which will then ask you (as your bank never will) for your full authentification details; and malicious code Trojans have already been mentioned. We know that there are a lot of computer viruses out there and there are different definitions of exactly what they are. If you have an infected machine there are a number of different payloads, key stroke loggers, things that can recognise when you are on a banking site, and all this was already mentioned. If you have stored sensitive personal details on your machine they can potentially search through your machine hard disk and see what they can find of potential interest to the fraudsters. There is also a third type, which is a lot rarer in the UK, which has the unfortunate name of "pharming" and that involves making alterations to the Internet infrastructure, particularly the domain name service system, to misdirect people who are attempting to go to their legitimate bank site.

Q108 ***Lord Paul:*** We have been told that one bank dominates the statistics. Is this true and, if so, which bank? We have also heard that the number of accounts compromised, and hence the amount of money at risk, is soaring. Do you have figures on this? Should we conclude that things could very rapidly get much worse?

Ms Quinn: As I was saying to my Lord Chairman at the beginning of our evidence, in fact there is no evidence to suggest that the figures that we will be publishing at the end of 2006 will be statistically in percentage terms much higher than the figures in 2005. That is not to say that we are in the least way complacent about this because fraud is still rising, but it is not rising at the level it had been rising. We do hold confidential data but we are not in a position to share that in open session. I may be prepared to share that if that would go no further through the Committee.

Mr Pemble: The Anti-Phishing Working Group statistics show that the primary targets worldwide for phishing still are eBay and PayPal, although there has been a general move towards attacking financial institutions, presumably because the fraudsters are able to get real money out of those. The other thing that has been seen is a quite significant rise in the number of different organisations being targeted. It is difficult to be precise but we are talking about, I think, 180 different organisations in a month. That is not evidence but it indicates that when the fraudsters start attacking an organisation, that organisation will quite quickly get up to speed with dealing with it, and certainly you are seeing attacks in America, which is still dominating the statistics, against smaller and smaller banking organisations. Obviously the UK banking community is not as fragmented as the American banking community.

Q109 ***Lord Howie of Troon:*** We have been told according to a survey that consumers feel more endangered by eCrime than by being burgled or mugged. First of all, is that true and secondly, if it is true, how are you responding to it?

Ms Quinn: I think the key is that it depends on the question you ask. We all get concerned about where we are talking about our own personal financial details. If we do bank on-line it is something we do regularly so it is very front of mind. If you are asked about the risk you might think in terms of the number of times I use my on-line banking service and therefore it is slightly more risky as I walk around very safe streets at night and I do not anticipate being mugged. I think if you asked people what they would prefer to happen to them that would be a different answer obviously.

Q110 ***Lord Howie of Troon:*** So you are not sure if it is true?

Ms Quinn: I think it very much depends on the kind of questions you ask. There is a level of fear that depends on the level of usage and the level of awareness.

Mr Whittaker: There are some very rich paradoxes out there. Sandra is absolutely right, it depends on the question you ask. If you go to the same people in one breath and ask them are they worried about security, they will quite clearly and reasonably have fears that they will wish to express. If you ask them in the following question how many people shop on-line, buy their groceries from an Internet merchant like Tesco, Sainsbury's or Asda, and have them delivered at home for ease and convenience, the same people will put their hand up and say yes. If you then ask them who banks on-line or has done a transaction on-line, they will put their hand up and say yes. It depends on what questions you ask and in what frame of reference you ask them.

Q111 ***Lord Howie of Troon:*** That is quite true but it is true of all surveys. Some people might ask, "Do you approve of Gordon Brown?" or, "Do you approve of that dreadful Scotsman Gordon Brown", and the answer might be quite different.

Ms Quinn: Absolutely.

Q112 ***Lord Howie of Troon:*** Do you believe it is true?
Ms Quinn: I think it is quite difficult from an organisational point of view to say one way or the other. The easiest way is to express it in personal terms. I do not feel as I bank on-line that this is the highest risk. I live in a very safe area and I take the normal personal security precautions that we all do. I think I would weigh up the fear of personal attack much higher than eCrime.
Lord Howie of Troon: So you are very sceptical about this conclusion and therefore you do not respond to it at all really? I do not blame you, by the way. Can I go on a bit. I am told that there is a system called universal two-factor authentication. I think Lord Errol mentioned it earlier on.
Chairman: Visa were just talking about the same thing.

Q113 ***Lord Howie of Troon:*** I must have missed that, Chairman. For the record, will you tell us what it is and, secondly, if this is a good thing, why has the industry in general not adopted it?
Mr Littas: We are adopting it. That is what Sandra explained a few minutes ago. "Two-factor" means something you have and something you know so you have a card and you know your PIN number. As Sandra explained, you put that PIN number in and get a unique, dynamic number used only once, which you put in the Internet transaction. Why has it not happened before? It is only fairly recent and the UK was one of the first countries in Europe to implement this technology because it is based on chip technology, so that is a condition for using this particular application.
Ms Alzetta: Just to add to that, we have just implemented Chip and PIN. The whole idea of using the dual-factor authentication is that we are using common specifications that have been developed, so that I can use my Visa card or indeed my card from another payment scheme and the reader will work for all the cards. That is really important because what that means is the clever bit sits in the chip on the card. The reader is just a device which anyone can use. If I forget it and I do not have it with me I can borrow yours or anyone else's. What it means is that it is much more convenient because we now have common specifications which are industry-wide specifications. We are not trying to compete in this area. It is an area of mutual interest to everyone.

Q114 ***Lord Howie of Troon:*** I think that was probably a very helpful answer as far as I am concerned. So I can take it that it is a good thing and that you are introducing it?
Mr Littas: Absolutely.
Lord Howie of Troon: Thank you, Chairman.

Q115 ***Chairman:*** That question was answered really by Visa. What are the banks doing? Are the banks going to provide the same sort of service?
Mr Whittaker: We developed, based on the MasterCard and Visa specs, a technical specification to allow the level of inter-operability that Sandra was describing to be achieved. We are discussing with our members who and which banks might wish to be adopting it and in what sort of timeframe. In the end it is for individual banks to make their own risk management decisions about what technology they employ. Some banks which may not be suffering very many losses at all might find the cost of the machines and the readers and that sort of solution as prohibitively expensive, bearing in mind the level of losses that they and their customers are suffering. It is an on-going debate at them moment within the industry. You have seen some press announcements from an institution in the UK saying they will be introducing them starting from next year and it will be interesting to see how many follow suit. As Sandra described, we do not regulate the industry and we cannot prescribe the solution. It is up to individual institutions to make their own risk management type decisions about what technologies they deploy to their customers and to decide what level of usability and cost-benefit they are going to get from a certain technology. We had the discussion earlier on about the technology that Alliance & Leicester have deployed. That was their response to their cost-benefit investment decisions for their requirements for their customers. Over time individual institutions will make their own decisions and those decisions will evolve as and when the cost-benefit case changes over time.
Ms Quinn: What is clear is that there is a great commitment within the industry to stronger authentication and different banks may adopt different approaches. What we want to make sure is that that operates for the convenience of customers and for the usability of customers because what you are going to be doing if you are giving devices out to individuals is asking people to have something else in addition to what they have got with them. When we introduced chip and PIN we were substituting a signature for a PIN so we were actually saying you do not need to do that any more, you need to do something else. What we are doing here is an additional layer of protection, and you will have a device, as Visa have demonstrated, and we need to make sure that customers will be able to use that and find it easy and accessible.

Q116 ***Chairman:*** APACS is a bank organisation; is that correct? So you represent the banks, you do not represent the customers. Is that why you are not prepared to tell us which are the bad banks and which are the good banks?
Mr Whittaker: I do not think there are any bad or good banks in this case.

Q117 ***Lord O'Neill of Clackmannan:*** Why do you not provide the information then? Why do you not make it public? You say it is commercial in confidence. Is there a legal obligation on you to stop you doing that or is it just that the people who own your organisation refuse to have the information made available?
Ms Quinn: We collate management information and statistics on fraud and have done for a long time for members and we do that and publish it on an industry basis.

Q118 ***Lord O'Neill of Clackmannan:*** That is not what I mean. If I am a customer and I am worried about going to one bank or another for on-line services, surely I am entitled to know which of them is the safest or safer than the other one in my high street?
Ms Quinn: The general point I would make is, exactly as Colin has said, there are no safe or unsafe banks.

Q119 ***Lord O'Neill of Clackmannan:*** But you would not tell us, that is what you are saying, you refuse to make public this information?
Mr Whittaker: We would therefore be forced to make a value judgment.

Q120 ***Lord O'Neill of Clackmannan:*** If you make the information available as a percentage of turnover, that stands for itself. It is not a question of you making a judgment. It is a question of you just having the guts to publish it.
Mr Whittaker: In the end, dare I say, with respect, it is not so much that the banks themselves or the banks' systems are insecure because those banks are not being attacked; it is their customers that are being attacked unfortunately, and the levels of controls that they are all deploying at the moment are broadly equal in the style of techniques they are using, and therefore trying to draw some sort of judgment or saying this bank is any stronger or any weaker or is suffering more losses or less losses than another bank does not help us describe why that bank is being attacked in the first place.
Lord O'Neill of Clackmannan: I am sorry, it is not up to you to make the judgment; it is up to the customer, and if the customer is denied the information then they are in no position at all to make a judgment.

Q121 ***Earl of Erroll:*** Can I ask a question which might clarify this which is: am I right in thinking that APACS is actually a banking trade body which has no responsibility whatsoever to the public and does not actually have any interface with the government or the general public? It is actually an internal banking body.
Ms Quinn: Can I say two things in response to that. You are exactly right, APACS is a trade association and we have 31 bank members and we work with them to co-ordinate the fight against fraud. What we are developing next year is a new government arrangement which is a new board which will replace what was formerly known as the OFT Payment Systems Taskforce and that is looking at exactly some of the issues that you are raising about increased transparency and increased awareness. I am sure they will be picking up those types of issues.

Q122 ***Lord Young of Graffham:*** I suspect my question is for Mr Whittaker, and thank you very much, it is a very interesting paper.
Mr Whittaker: Thank you.

Q123 ***Lord Young of Graffham:*** Let us assume for the moment that I have lost money from my account in some way or another. At the moment all banks will refund that amount of money. You say on page four of your submission that banks currently choose to refund money. Is there a legal obligation to refund or is it a matter of goodwill?
Ms Quinn: There is no legal obligation. The key is that all banks publish very clear guarantees on their websites to customers that if customers operate within their terms and conditions then they will refund any losses they have. It is one of the things we are looking at through the Banking Code. The Banking Code sets out standards of good practice against the industry and that is currently going through a review process. It gets reviewed every three years. We have just started the review process for the edition that will be current in 2008. I think it is fair to say that one of the aspects I expect we will get comments from stakeholders on is to tighten up some of the fraud guarantees provided within the Code. I think it is the level of awareness that we need to look at.

Q124 ***Lord Young of Graffham:*** Can I just take that a bit further. If I lose my cheque book or somebody steals my cheque book and forges my signature, I get my money back from the bank?
Mr Whittaker: You do.

Q125 ***Lord Young of Graffham:*** If somebody takes my credit card and forges my signature the credit card company gives the money back. Are you saying that

only in the case of on-line transactions the bank is not obligated to give me my money back?
Ms Quinn: There is not an obligation in the Code. In both the other instances you suggest there is an obligation in the Code.

Q126 ***Lord Young of Graffham:*** Do you think that is appropriate?
Ms Quinn: I think it will be something looked at in the review process next year and it will be very interesting to see what the outcome of that is.

Q127 ***Earl of Erroll:*** Do you think we should replicate something similar to the Bills of Exchange Act 1888?
Ms Quinn: 1882.
Earl of Erroll: It is my memory!

Q128 ***Lord Mitchell:*** He was there for the third reading!
Ms Quinn: I think one of the things that is changing is the rules about cheques. At the moment we have in the UK nothing about certainty of cheques, so if I give you a cheque and that turns out to be fraudulent, but in good faith you have banked it and you have withdrawn the funds, if it subsequently turned out to be fraudulent even two or three weeks later, your bank could take that money back off you even if you have spent it. What we have just published is a guarantee that as long as you have not been complicit in the fraud that is committed, six days after you have deposited that money that money will definitely be yours. That will be a change in the cheque arena. One of the things I would mention about the Banking Code is the key responsibility it places on the banking industry. The burden of proof lies with the industry to prove that a customer has been negligent and, as you can imagine, in terms of customer service you want always to be relating well to your customer and believing what they tell you.

Q129 ***Earl of Erroll:*** And that is a change from the early days when banks refused to refund people who had had money withdrawn from ATMs, and that is going to stay that way?
Ms Quinn: There is no doubt that that is not going to change.

Q130 ***Lord Harris of Haringey:*** Could I address a question to Mr Littas. A week or two ago Visa contacted me—I am sure it happens to everybody—with a suspected fraud on my credit card and we sorted it out, and then they started selling me identity fraud protection insurance, which initially sounded quite a good idea, but I thought about it afterwards and I thought, "No, this is all wrong." It is the same issue that is coming up. There is a problem and they are trying to sell you insurance at the same time. Is this going on? Is this a general situation or just a Visa situation?
Mr Littas: To start with, the company that contacted you was not Visa. We do not contact individual card holders so it must have been the bank that issued your particular credit card who did that.

Q131 ***Lord Mitchell:*** Barclays.
Mr Littas: They may have acted upon information that we provided of a suspect transaction, but that relationship of how a bank deals with its card holders is entirely the bank's responsibility. We do not deal with merchants or with card holders.

Q132 ***Lord Mitchell:*** Alright, somebody contacted me.
Mr Littas: And no doubt it was the bank that issued your credit card.
Chairman: I think we must move on. Lord O'Neill?

Q133 ***Lord O'Neill of Clackmannan:*** When on-line banking started and when IT was applied in the last five years, we were sold the idea in terms of increased efficiencies and things like that but also it was going to be cheaper, and to an extent that is reflected in the fact that if you have deposit accounts on-line they tend to afford a higher degree of interest. Do you think that there is a danger now that the public see on-line banking as something that affords a higher rate of interest and the banks themselves see it as a kind of cheap option? You do not have the branch infrastructure to worry about. You barely have, in most instances, even the call centres—God forbid—to worry about. Do you think that there ought to be an added dimension of the local branch so that you can go in there on occasion or would that destroy the economics? It has been suggested that if there was a branch dimension you could end phishing at a stroke.
Ms Quinn: Not being a bank ourselves that is really a question for a specific bank to answer. One of the parallels I would draw is there has been a lot of discussion over the last two or three years about the diminution of free-to-use cash machines in areas of deprivation. There has been an announcement today where a number of banks have clubbed together and agreed to provide 600 more free-to-use cash machines, and that is an area that banks continually look at. The key drivers here are things like financial inclusion, making sure those people who need access to a bank branch have access to a bank branch, and that is a different issue I think to the Internet *per se*.

Q134 ***Lord O'Neill of Clackmannan:*** I take the point about the social banking dimension and there are other pressures on the banking system to address that. It is really just this question that it would appear

that a lot of the financial planning of banks in terms of service to customers has been based on the assumption that Internet banking could afford great savings but some of these savings have a security downside. Do you think that, for example, if the branch had a bigger role, phishing could be eliminated or, alternatively, maybe if branch marketing departments stopped sending emails then they would not be quite as vulnerable to phishing expeditions as they are at present.

Ms Quinn: I think that last point is particularly valid in that there is a balance, is there not, between the marketing a bank wants to make of its services, and it wants to deliver those marketing messages through email or ways that it knows its customers reads its material, and the kind of information we receive through phishing emails. That is one of the reasons at industry level we have made some very clear messages such as your bank will never ask you to access your website through a link in an email. That is a very clear message we promote for exactly that reason. Unfortunately, there is a balance between marketing and security.

Q135 ***Lord O'Neill of Clackmannan:*** One last point, you mentioned the Banking Code and you say it is a triennial review. Given the dynamic of your industry at the moment and the rate of change, do you think that three years is maybe too long a period to carry out this review and that it should be every 18 months or something like that because there seem to be changes happening so dramatically?

Ms Quinn: I think that is a really fair point. What we have done is we have changed the Banking Code review period from two years to three years, but what we have is an interim review process so if there is something where customers are at a disadvantage there is a process in place where we can have an interim review specifically about one topic and then the change will become effective immediately.

Q136 ***Lord Mitchell:*** We just wanted to know the level of international co-operation between financial institutions who are looking at eCrime.

Mr Whittaker: It is quite profound. We are very fortunate to have established an excellent relationship with the Australian banks. They were the first banks who were attacked in a significant way. They developed a co-operative relationship dealing with these issues and we learnt a lot from them to start off and we formed a united front in discussion with international law enforcement as well. We have broadened that out recently to encompass some American banks, German banks, Dutch banks, Danish banks around the world who are suffering these sorts of attacks. Everyone is learning from the lessons of people who suffered the hardest knocks first, which unfortunately was Australia and the UK.

Mr Littas: Of course Visa is all about international co-operation and part of that co-operation is to fight fraud. I think we have come a long way from a few years ago. Based on the fraud numbers which have been constantly on the decrease for the last 10 years, we have now record low fraud levels in Visa of five basis points, which is five pence on every £100 turnover, and that is thanks to that co-operation you asked about. We do co-operate better, we do things better, and we try to introduce standards and systems with global application.

Q137 ***Chairman:*** Have there been any successful attempts to approach agreement with Eastern European countries or with Nigeria for example?

Mr Pemble: There are a number of international co-operation agreements. Obviously it is relatively difficult for financial organisations—and it should be—to undertake law enforcement action themselves. Therefore it is dependent upon the financial organisations working with their local law enforcement who can then go through co-operation agreements with the international law enforcement authorities. Certainly the National High Tech Crime Unit, as was, had a number of successes in the former Soviet Union and the Met Police Operation Sterling team have done a considerable amount of work with the Nigerian authorities. There is considerable co-operation through organisations such as FIRST and the G8 Line Group and obviously Interpol and Europol, between the law enforcement bodies, bringing them together to establish relatively simple pathways for financial organisations and their customers to report fraud. Clearly, international legal co-operation can be slow. Mutual legal assistance treaties move at the speed of diplomacy not necessarily at Internet speed. I think it is an important question to be asked as to how from a legislative/international law point of view this can be improved. More research is needed and possibly along similar lines to the CTOSE[1] programme that was run by the European Union a couple of years ago, which as well as including European Union nations did include the United States National Institute of Standards and Technology as well as law enforcement organisations from around the world. There needs to be greater involvement from the commercial sector. ENISA, the European Network and Information Security Agency, might be an appropriate body to lead that or there maybe other organisations which can pick that cudgel up.

[1] http://cordis.europa.eu/fetch?CALLER=PROJ_IST&ACTION=D&RCN=60288

Mr Littas: On international co-operation we were successful—and I mean by "we" the payment card industry—in working with Interpol on the problem of counterfeiting which has now very much reduced as a problem. I met Interpol only last week to try to get them involved on other types of fraud, in particular "card not present" fraud which is a growing type of fraud worldwide. We have certainly provided funding and training and support to Interpol on counterfeiting but our offer last week was we wanted to do the same thing with regard to card not present fraud because that is clearly something we want to tackle head on.

Q138 ***Lord Harris of Haringey:*** In some US states there is a legal obligation on businesses to notify customers and others of security breaches. Should we have that sort of legislation here?
Mr Pemble: It is an important question to consider but it is also important to note that there are considerable differences between the US state bills. The results have been far from uniformly positive. There are a relatively large number of potential breaches reported under the US rules primarily of things like laptop thefts, where there is a very, very low risk of subsequent identity compromise. Also there are a significant number of actual compromises that occur that are only noticed once the fraud starts taking place. There is also the point that the obvious reputational impact on an organisation that makes a report is likely to lead organisations to concentrate to a very great degree on the PR and media management of the incident which will detract resources from managing the problem. There is also a particular problem in the payment cards area, as was mentioned. It is difficult for the organisation that actually suffers the breach to have that direct relationship with the customers.

Q139 ***Lord Harris of Haringey:*** Sorry, they are my details that are potentially being breached; should not the organisation holding them have an obligation to inform me of that possible breach?
Mr Whittaker: There are implied obligations under the Data Protection Act 1998 which does call for data processors and data controllers to make that judgment call. However under UK law and under the Data Protection Act, it stresses throughout, when it comes to the control measures, the importance of making security and risk management decisions based on your understanding of the level of harm that could give to the data subject. That is the right and responsible way to go about the issue. Certainly when you talk to US commercial enterprises and institutions who are suffering these independent state legislations out there, there is some concern that as well-intentioned as the legislation is (which it is and everyone would applaud it) it does cause its own level of unintended consequences. One of those is to increase anxiety. Because the enterprises have got no ability to form a discretionary view on the level of harm that compromise might cause, and as you heard some compromises are trivial but you still have to let the consumer know, so consumers are being bombarded and in some cases are being warned up to five or six times when there has been a data compromise, and they cannot easily sort out themselves the impact that any one of those sorts of cases is going to cause them. Therefore there is a good argument for saying if you are going to do this thing, do it in a much more appropriate and responsible way, making informed decisions about the level of harm that could be incurred.

Q140 ***Lord Harris of Haringey:*** It does sound to me as though what you are saying is that these decisions are actually taken in terms of whether or not it is going to damage the image of the institution concerned.
Mr Whittaker: I did not say that.

Q141 ***Lord Harris of Haringey:*** I am saying that is what it sounded like. Could I ask specifically whether in cases where there is some form of security breach which has been initiated fraudulently, say by an employee, it is always the practice of the institutions concerned to notify the police?
Mr Whittaker: By and large yes it is.

Q142 ***Lord Harris of Haringey:*** Could we be told whether it is normally the practice where there is some form of security breach for the institutions to notify ENISA?
Mr Whittaker: Not necessarily. ENISA are involved with critical national infrastructure.

Q143 ***Lord Harris of Haringey:*** Financial institutions are part of that.
Mr Whittaker: Yes they are but at the moment ENISA are concerned with critical national infrastructure incidents and issues. It is not their responsibility to deal with levels of fraud.

Q144 ***Lord Harris of Haringey:*** I was talking about a security breach and I am concerned. You say that it is not significant that a laptop has been stolen. Nationwide lost a laptop and that put the personal data of 10 million customers at risk. That was not reported for several weeks but in the end I think Nationwide did write to people about that.
Mr Whittaker: Yes.

Q145 ***Lord Harris of Haringey:*** Why did they leave it so long?

Ms Quinn: I am afraid you would have to ask Nationwide that question. That was a decision they made.

Q146 ***Lord Harris of Haringey:*** What do you think is good practice?
Ms Quinn: Assessing the risk, assessing what kind of information customers would find useful. I think the best way of doing that is asking customers what kind of information they would find useful. It is very easy to make judgment calls about what we think a customer might find useful but the best way is to ask customers themselves. If you go back to the US case, there is a very different regulatory regime around there as well in that if you have been a victim of fraud you do not always get your money back whereas in the UK you have as a backstop that if you have been a victim of fraud you will be recompensed. That is not always what happens elsewhere.

Q147 ***Lord Harris of Haringey:*** Could I ask Visa how many security breaches your organisation has had in the last year which have been initiated by your own employees?
Mr Littas: Internal fraud?

Q148 ***Lord Harris of Haringey:*** I am interested both in internal fraud but also in inadvertent security breaches which have made the system vulnerable.
Mr Littas: We did not have any security breaches internally. We have had a number of breaches of security in various entities where Visa account data was compromised which we subsequently told the banks about. We had quite a substantial number of those breaches.

Q149 ***Lord Harris of Haringey:*** Could you give me an example of what that sort of thing might mean?
Mr Littas: It might mean that a hacker getting into a merchant's database, taking that data and then using it for fraud, in particular card not present fraud, because they steal the account data that enables them to use that data to do fraud on the Internet, so that is a problem. So we had a number of breaches.

Q150 ***Lord Harris of Haringey:*** Can you give us some indication of the number?
Mr Littas: I can give an exact number. For the last year we had well over 100 breaches affecting European cards. We actually only had 10 hacks in Europe affecting Visa Europe cards. Most of these hacks take place in the US and then the data is sold on the Internet or in other ways and then used fraudulently, both face-to-face and in particular on the Internet for purchases.
Chairman: Lady Hilton has a question on this subject. Would you like to ask that now.

Q151 ***Baroness Hilton of Eggardon:*** I think effectively it has almost been answered but what steps do you take to encourage your merchants to ensure that it has security and do you have any sanctions if they fail to maintain the right level of security?
Mr Littas: We have a programme which we call the account information security programme which in fact is based on a standard agreed in the whole payment card industry—the payment card data security standard—and we are implementing that. It is a requirement both for merchant processors and everybody who holds Visa or any organisations' payment card data to introduce those measures, to protect data for the card owner, to avoid hackers going in—for example effective fire walls or encryption or whatever is necessary to protect that data. That is a programme that has been in place for a couple of years and we are implementing that, together with the rest of the payment card industry.

Q152 ***Baroness Hilton of Eggardon:*** If you find merchants who are not applying appropriate levels of security, do you drop them in some way or remove their ability to get payments by Visa?
Mr Littas: The sanction would be, which has been clearly outlined in that programme, if a merchant does not comply with those rules and there is subsequent fraud, that merchant or the acquiring bank will then be liable for that fraud. We can also penalise merchants via the acquiring bank who clearly are out of order with these rules.
Mr Pemble: It is a requirement upon the acquiring bank who are providing the merchant with the transactions to ensure that the merchant provides evidence of the level of compliance with the payment cards industry's standards. They have been recently updated. There is now version two out and it does lay down a number of steps—regular security testing, the use of encryption, and not storing particularly sensitive data. That is a publicly available standard and set of tests that anybody can get off the Internet.

Q153 ***Baroness Hilton of Eggardon:*** My understanding from the banking sector is that you have not had any examples of personal data being hacked into.
Ms Quinn: No, we are not aware of any case in the UK.

Q154 ***Lord Harris of Haringey:*** Would you be told?
Mr Whittaker: Yes.

Q155 ***Earl of Erroll:*** This is encryption inside the database at the field level, so in other words it is not worth stealing the information; or is it sitting there unencrypted at any point?

Mr Pemble: Certain field data in the database is required to be encrypted.

Q156 ***Earl of Erroll:*** If you insist on this then it is not worth stealing the databases?
Mr Pemble: A direct disk-to-disk copy of the database would not be useable for direct card not present fraud.

Q157 ***Earl of Erroll:*** So do you insist on this with all merchants?
Mr Littas: We do not insist on encryption; we insist on protection such as putting a fire wall in front of the server to make sure that the data cannot be hacked. Encryption is not required as yet. This is one of the things we are thinking about introducing but it is not required for now.
Chairman: We have almost run out of time but Lord Young has a question.

Q158 ***Lord Young of Graffham:*** Just one quite quick question regarding Visa. I understand Visa has banned the use of credit cards for the purchase of child abuse images. How can they police that? How do they know that an on-line transaction takes place or if they can, would you see this as being widened so that you could find more and more transactions being banned?
Mr Littas: Is it a question about whether we plan to extend this system?

Q159 ***Lord Young of Graffham:*** Yes, first of all, can you do it effectively?
Mr Littas: Absolutely. I think we can say that the co-operation with the Child Exploitation and On-line Protection Centre that we conduct has been very, very effective. They have an intelligence section and they find suspect sites very, very rapidly and they work with law enforcement and other entities to close these down. I think we can say that that has been really very effective. Whether we are going to extend that to apply to other services or goods, we are certainly looking at everything. We do not want Visa cards to be used for any sort of immoral or illegal activities obviously, but right now we do not have any plan to extend that approach because the law of the land is really taking care of most markets.
Ms Alzetta: Our position has always been that it is not our job to be the moral arbiter. However, the reason that we made an exception for the child abuse images is because, sadly, the fact is that law does not exist in all countries that prohibits this so we have taken the step of saying we are just not going to allow it.

Q160 ***Lord Young of Graffham:*** The only way you can attack it is from the credit card side?
Ms Quinn: Can I just add that one of the things that happened this year is that the House of Lords changed the legislation on the Data Protection Act to allow the Child Exploitation and On-Line Protection Centre to share data with the banking industry about those people prosecuted for buying illegal images on-line with their credit or debit cards, so that we can now be passed information about the credit or debit card used so the banking industry now knows about it to make sure that card is taken away from the perpetrator.
Mr Pemble: You will also be aware that there have been recent changes in American legislation with regard to on-line gambling. The ban of the acceptance of credit card payments from American citizens has meant that all of the on-line gaming facilities, and subsequently the banks that acquire their credit card transactions from them, have had to change their systems to comply with US law. So it really is a matter of complying with the law of the various countries. Individual banks, as opposed to the card schemes, may very well have an ethics policy which may be much tougher than the law. To mention a name, the Co-operative Bank in the UK markets itself as an actively ethical bank so you would expect their internal rules to be slightly different.

Q161 ***Earl of Erroll:*** It is back to co-operation with law enforcement—if something like the National e-Crime Unit was to re-emerge now that the NHTCU has been overtaken by SOCA, would you be interested in collating small-scale incidents and analysing them and giving intelligence to such a unit?
Mr Whittaker: Very much. We saw the recent announcements by Commander Sue Wilkinson of the Met, who is the ACPO lead on eCrime, who was making some very positive suggestions on the need for a UK national centre of excellence now the NHTCU is no longer there to co-ordinate activities. We think that is a very worthwhile and very useful proposition and one which we would support and contribute to and co-ordinate with.
Mr Pemble: The banks do share intelligence data with SOCA eCrime and with the SCDEA in Scotland. It is not always possible for police resource to be put into criminal investigations, that is a matter for society, but there is no hiding of fraud to that extent. A lot of information is shared with the police for them to make use of in intelligence and statistical work as opposed to specific criminal investigation.
Chairman: On that positive note that there is some collaboration, let me thank you all very much for answering all these questions. We have had a lot of questions and you have answered them clearly and well and we very much appreciate it. We very much appreciate your time and your coming to talk to us, so thank you all very much.

13 December 2006

Memorandum by the Financial Services Authority

Introduction

1. The FSA submits this memorandum in response to the Committee's call for evidence on its inquiry into personal Internet security. The memorandum:

- sets out the legal basis and regulatory objectives of the FSA and the extent and nature of our interest in personal internet security;
- describes work we have done in the past in areas related to personal internet security, such as cybercrime and information security; and
- outlines the further work we are planning in these areas.

Background

The FSA is the single statutory regulator for the great majority of financial services in the UK. Its powers are conferred primarily by the Financial Services and Markets Act 2000 (FSMA).

2. FSMA requires the FSA to pursue four objectives:

- maintaining market confidence in the financial system;
- promoting public understanding of the financial system, including awareness of the benefits and risks of different kinds of investment or other financial dealing;
- securing the appropriate degree of protection for consumers, while having regard to the general principle that consumers should take responsibility for their decisions; and
- reducing the extent to which it is possible for a regulated business to be used for a purpose connected with financial crime, such as money laundering, fraud and market abuse.

3. In carrying out these functions FSMA requires the FSA to take into account a number of matters, which we refer to as "the principles of good regulation". These are:

- the need to use its resources in the most economic and efficient way;
- recognising the responsibilities of regulated firms' own management;
- the principle that the burdens and restrictions imposed by regulation should be proportionate to the benefits;
- the international character of financial services and the desirability of maintaining the UK's competitive position;
- the desirability of facilitating innovation;
- the desirability of facilitating competition; and
- the need to minimise the adverse effects of regulation on competition.

4. The FSA is a company limited by guarantee and is financed wholly by levies on the regulated industry; it receives no Government funds. The FSA's governing body is the Board, all Board Members are appointed by the Treasury. The Board sets overall FSA policy. Day-to-day operational decisions and management of staff are the responsibility of the Chief Executive. The FSA is accountable to Treasury Ministers and to Parliament. The legislation requires us to report annually to Ministers on our discharge of our regulatory responsibilities, and Ministers are required to lay our Annual Report before Parliament. The Treasury Committee of the House of Commons takes evidence from us regularly, on our Annual Report and other matters.

5. In discharging all our responsibilities, we work closely with Government and other authorities and agencies that have related responsibilities. In the case of personal internet security we are starting to work with the Information Commissioner's Office and with the regulators of other sectors of industry such as the Office of Gas and Electricity Markets (Ofgem) and the Office of Communications (Ofcom). Our work with the Home Office in this area is set out in paragraph 20.

FSA Work on Areas Related to Personal Internet Security such as Cybercrime

6. Personal Internet security is an important issue for the financial services industry, as ever-increasing numbers of firms seek to exploit the cost savings, customer convenience and flexibility that the internet offers. Our interest in this issue derives from all our regulatory objectives: the reduction of financial crime, consumer protection, consumer awareness, and market confidence.

7. Increasingly, both organised and opportunistic criminals are stealing customer data. The theft may either be from the customer's PC, using malicious software or "phishing" attacks or from financial institutions or retailers who hold financial data for payment purposes, using hacking techniques or insiders to steal the data. Customer data can then be used to carry out various forms of identity theft, ranging from relatively simple fraudulent use of card details to much more sophisticated account takeovers. Even small amounts of seemingly non-sensitive customer data can be used to obtain false documentation. This can be used by criminals to facilitate identity theft and ultimately obtain credit and other products in the victim's name. The market in which stolen personal data is traded by criminals, particularly on the internet, has matured. It has features such as discounts for large amounts of data and "feedback" scoring on the quality of data sold, in much the same way as legitimate sellers are rated on eBay or other legitimate internet sites.

8. Large-scale compromises of customer data from both financial services firms and non-financial, retail-focused businesses are of particular concern. In the past few years, organised criminal gangs have both corrupted and coerced individuals in financial services firms and infiltrated firms with their own people in order to access the large amounts of sensitive data they hold. Although we have no direct information on firms outside those we regulate, it seems likely that this is also happening in non-financial services firms.

9. In pursuing our statutory objectives we seek to ensure that firms—both at the authorisation stage and on a continuing basis—have the necessary systems and controls in place to meet the requirements of the FSMA (the "threshold conditions") and in our Handbook of Rules and Guidance. This includes assessing whether their systems and controls are adequate to prevent them being used for purposes connected with financial crime, including fraud; it also includes the adequacy of their information security measures. We are also concerned to ensure that the persons running the firm are competent and committed to conducting their business with integrity and in compliance with our regulatory requirements.

10. We are a risk-based regulator, so we seek to assess whether firms' systems and controls are appropriate for the business they conduct, rather than assessing all firms against a single model. In evaluating, and seeking to mitigate, the risks in firms that provide online services, we are likely to focus in particular on areas such as information security, disaster recovery and anti-fraud measures. Where firms provide cross-border services, we co-operate closely with overseas regulator in our supervisory activities.

11. Where we identify weaknesses in firms' systems and controls, we use a variety of methods to raise standards. Most of this work is done in private, for example, through discussions with firms' senior management on remedial action or more formal "risk mitigation programmes". Our enforcement powers enable us to conduct investigations, to take administrative and civil action, and to commence criminal proceedings. For legal and policy reasons, we usually comment in public on individuals or firms only where, after due process, a sanction (criminal or administrative) has been imposed. In terms of disciplinary sanctions, we have statutory powers to censure firms and individuals publicly or to impose financial penalties on firms and individuals. The ultimate regulatory sanction available to us is to withdraw our permission for firms to carry on some or all of their regulated financial services activities, or to prohibit individuals from working within the industry, either at all or in connection with specified function(s) for a fixed or indefinite period.

12. We also conduct "thematic work" on particular risks we have identified that affect groups of firms, sectors or even the entire financial services industry. We normally publish the aggregate results of this type of work. Our thematic reports generally contain good practice observations and cite areas where firms could improve their practices. This type of work is often used for financial crime issues, given that financial crime can affect all the firms we regulate. Thematic work also allows us to identify problem areas or sub-sectors in the broad range of firms we regulate.

13. In order to assess the risk of customer (and other) data being compromised in financial services firms, we conducted some thematic work in 2004 and published a report "Countering Financial Crime Risks in Information Security". We found a mixed picture of how financial services firms were managing their information security at that time. Although some major firms, particularly in the banking sector, had built their defences in response to targeting by hackers and fraudsters, other sectors and small and medium-sized firms were less well-prepared and risked exploitation by criminals seeking a weak point in the system. Although we found that known financial losses to firms and customers were low, we encouraged firms to do more to address the

potential risks rather than responding to attacks once they have occurred. We recognised the inherent difficulty which firms face in keeping up with rapidly evolving technologies and increasingly determined, dynamic and well-organised fraudsters. We also highlighted that consumers must protect themselves by safeguarding their personal details or following the security tips offered by the firms with which they deal.

14. In 2005, we conducted some work on the offshore operations of 15 large financial services firms, which looked at several issues including information security. We observed a high level of security in operation; indeed, some firms said that the security measures in place in India were better controlled than in the UK. Examples of security measures in place in some offshore operations included:

- Swipe entry to the premises and further swipe card restricted access to specific client areas.
- CCTV and/or security guards walking the floors.
- Staff prevented from taking personal effects to their workstation.
- Computers without hard drives, floppy drives, USB ports, access to email/internet or printers. Where printers were required, access was controlled and restricted to relatively senior people.

In all companies reviewed, data was stored onshore in the UK and transferred to India as necessary. Firms had also implemented systems to monitor telephone conversations, protect data and monitor staff. There was no evidence to suggest consumer data were at greater risk in India than in the UK.

15. In addition, new methods being tested in the UK by banks to improve internet banking security include two-factor authentication, where users are required to enter two means of identification: one is typically digits from a physical token and the other is typically something memorised. Another bank has recently started to offer free anti-virus software with its online banking service.

16. In a speech to the British Bankers Association's Annual Financial Crime Conference on 5 December, Philip Robinson, the FSA's Sector Leader for financial crime, discussed the issue of information security and the FSA's work in ensuring that firms have appropriate systems and controls in place[5].

Consumer Information

17. Consumers have an important role to play in protecting their personal internet security. We have emphasised to banks the need to engage consumers in their work to combat the rise in online banking fraud. We carried out consumer research in October 2005 to gauge confidence in internet banking. The research found that consumer confidence in internet banking was fragile. Half of active internet users said they were "extremely" or "very" concerned about the potential fraud risk of making an online transaction. Most consumers who conducted online banking were taking steps to protect themselves against fraud by installing security software on their PCs, but over a quarter either did not know when they last updated their software or updated it infrequently. Our research found that, if banks were to tackle online banking fraud losses to them by shifting the liability fully towards the consumer, more than three quarters of users would abandon internet banking. 95 per cent of users surveyed believed that at least some responsibility for security should lie with the bank, while 45 per cent believed banks should take sole responsibility.

18. Regulated firms already have the normal commercial incentives to manage their fraud risks. Our approach to combating fraud is therefore to add value to what firms are doing by working in partnership with other stakeholders to ensure that firms have access to the knowledge and tools they need. In line with this approach, we work with trade associations, law enforcement and Government (including Her Majesty's Revenue and Customs, the police and the Serious Organised Crime Agency, whose eCrime unit has particular expertise on high tech crime), other regulators (including the Office of Fair Trading and The Pensions Regulator, which will have anti-money laundering responsibilities under the 3rd Money Laundering Directive) and firms to mitigate information security risk.

19. The Banking Code Standards Board (BCSB) is responsible for overseeing the way in which banks conduct their business and the FSA ensures that banks put into place appropriate systems and controls to prevent fraud.

20. Through our consumer website we alert consumers to a variety of scams, including phishing and advance fee fraud, and provide information on how consumers can protect themselves from identity theft and what to do if they become victims. In addition, we sit on the Home Office's ID Fraud Steering Committee and its subgroup, the ID Fraud Consumer Awareness Group. We have contributed to their "Identity Theft—Don't

[5] Philip's Robinson's keynote address to the British Bankers Association's Annual Financial Crime Conference, delivered on 5 December: http://www.fsa.gov.uk/pages/Library/Communication/Speeches/2006/1206_pr.shtml

Become A Victim" public awareness campaign. Financial services and other firms have ordered about 11 million leaflets from this campaign for distribution to customers. Initiatives such as the "Get Safe Online" campaign run by the Government in collaboration with the private sector also contribute to consumer education in the area of personal internet security.

Future FSA Work on Cybercrime and Information Security Issues

21. In view of the pace of technological change and the dynamic character of organised fraud we keep information security issues under close review. In the past year, the media have reported several significant incidents of data loss and/or lax information security. Although some of the cases reported related directly to financial services firms, others appeared to derive from companies in other sectors of industry which hold consumers' financial information for payments purposes. In these cases, the fact that bank account and credit card information has been compromised, coupled with the manner in which the media sometimes reports these incidents, can lead to the perception that the compromise was the bank's fault. And, whatever the source of the compromised data, the subsequent attacks on individuals' bank or credit card accounts affect firms regulated by the FSA, as well as their customers.

22. We are currently conducting a project examining the methods used by financial services firms to authenticate the identity of consumers during remote contact (for example, via telephone or internet), and how this data is protected while held by the firm and its agents. In line with the approach outlined earlier, we plan to publish the results of this work by mid-March 2007.

23. We are still finalising our work programme for the next financial year. In the area of personal data security we are currently considering taking forward a number of strands of work. The areas we are looking at are:

- Offshoring: In evidence to the Treasury Committee in October we undertook to look again at the financial crime and information security risks associated with the offshoring of significant functions in financial services firms, in the light of that Committee's concerns over recent media reports.
- The security of consumers' banking data held outside the financial services industry: We intend to meet the Information Commissioner, relevant regulators such as Ofcom and Ofgem, and other bodies to discuss measures to improve the security of banking information in sectors outside the FSA's regulatory scope.
- Low tech information security risk: We will study the potential for low-tech breaches of information security (for example, careless disposal of sensitive consumer data; the removal of sensitive consumer data from the workplace; staff awareness of information security issues etc), and the systems and controls firms have in place to mitigate such risk.
- Identity theft risk arising from financial marketing practices: This project will consider issues such as the appropriateness of marketing literature which contains non-essential, and sometimes sensitive, consumer data, such as unsolicited credit card cheques and partially completed credit application forms, and also the inclusion of sensitive personal information in other types of communications from forms such as pension statements.

8 December 2006

Examination of Witnesses

Witnesses: Mr Philip Robinson, Sector Leader, Financial Crime Team and Mr Rob Gruppetta, Financial Crime Team, Financial Services Authority, examined.

Q162 ***Chairman:*** Mr Robinson and Mr Gruppetta, thank you very much for coming to talk to us and answer our questions. Would you now like to introduce yourselves and then make any opening statements should you wish to do so.

Mr Robinson: My name is Philip Robinson and I am the Director of Financial Crime in the UK's Financial Services Authority.

Mr Gruppetta: My name is Rob Gruppetta and I work at the FSA with Philip on his Financial Crime Team.

Mr Robinson: We have no need to make a statement.

Q163 ***Chairman:*** Let me start out with a simple question: how secure is on-line banking?

Mr Robinson: You have heard a lot of evidence already about that. Our view is that it is very secure generally because it often requires more security than non-on-line banking. There may be questions about how the security is used, but certainly where you require somebody to have to deliver some security

password to get access, that is generally more secure than other mechanisms of payment in cash.

Q164 ***Chairman:*** Do you bank on-line yourself?
Mr Robinson: I do, sir.
Mr Gruppetta: So do I.

Q165 ***Chairman:*** You make payments et cetera, as well as just monitoring your account?
Mr Robinson: I do. I often make payments very late at night, often when my daughter has asked me to top up her bank account at university, as we have all done, so I am certainly a very active user of on-line banking facilities.

Q166 ***Chairman:*** There is general agreement among those who have submitted evidence to this inquiry that the current reliance on shared secrets for on-line security is wholly inadequate. What pressure has the FSA been putting on the industry to raise security to more acceptable levels?
Mr Robinson: In 2004 we actually reviewed the information security issue from a financial crime perspective, and we have mentioned that in our submission. What we found in 2004—and I will talk in a minute about what we have done in 2005 and what we will do in the future—was that in general the very large institutions were very up to speed and they were aware of the threats and risks. They had very strong disciplines in managing their IT and in the environment that we saw at the time we felt that the large institutions did well. We found though that the middle-sized and smaller institutions just did not have the same rigour of practices. We publicised that information in 2004 and we followed up with one or two other interventions in 2005 and 2006 to make sure that the issues were being addressed. As a risk-based, proportionate regulator, our starting point is always to look at the systems and controls that firms are implementing. Indeed, that is our requirement under the Financial Services and Markets Act. We are not a direct regulator of the behaviour of the banks, for example, towards their customers; that is the Banking Codes Standards Board. So our starting point is are the firms managing their financial security risks properly and, if not, what are they doing about it? We publicise good and bad practice and we followed up on that information through our supervision of banks through 2005 and 2006.

Q167 ***Chairman:*** So can we expect to see Chip and PIN style authentication—what Visa call dynamic pass code authentication—generally available for on-line credit cards and, if so, when do you think it will be widespread?
Mr Robinson: I think that we need to make a distinction between on-line payments for purchases —there are around 26 million individuals who do that sort of thing—and people who have on-line bank accounts. The difference in the nature of those two relates to the way you can communicate with the customers. If you have got an on-line bank account many of the alerts and other concerns that people were talking about earlier on can be brought to people's attention if they are going to go on-line. There are various other ways of doing that. If you are dealing with people who are making on-line payments with a credit card, they may not have an on-line bank account and they may not themselves therefore get access to these on-line warnings, and other things may be necessary. The reason I made those comments in that way is really that you need to focus on the risk that is being presented. The two factor authentication already exists in many areas with the existence of a Chip and PIN card and the knowledge of a PIN. The problem with that is that in the area of customer not present fraud, which you have heard is a growing area, and I would say is one of the larger growing areas in fraud of that nature, you do not have the capacity to put that two factor authentification into play unless you have some other mechanism. It is my judgment that that is the direction in which the industry will go. Our starting point is that we would not necessarily instantly require institutions to do anything. Our starting point would be to ask the question "are they managing the risks that are presented by their channels of operation?" So a bank that is not offering, for example, an Internet banking opportunity—and there are many that are not—would not need to have that level of protection. A bank that did might feel that it was appropriate to do that or it might want to do some other level of protection. Really we would be looking at whether institutions are managing the risks presented by their propositions to customers and the nature of their experience, are their fraud losses going up or are they being managed well.

Q168 ***Earl of Erroll:*** Of course the banks are offloading a lot of risk onto the merchants. Is the risk actually being taken in the right place or should the banks be taking the risk because they are the people who might be able to do something about that?
Mr Robinson: I think our very clear view as the FSA is that in a world of electronic commerce, particularly on-line banking but it would apply in every respect, you need to have a shared responsibility. The sharing should be between consumers, merchants (in the case being talked of here) or third party acquirers of personal data, and the banks themselves. So it is a shared responsibility between the bank, the third party and the customer. I do not think it is possible to make that responsibility exist in any one area because the very nature of the electronic channel is that it is an open network and it is susceptible to compromise at the weakest link. You said, I think,

that banks are moving the liability from themselves to the merchants. That may be a matter that you would wish to discuss with the banking sector as a whole. From my side, we are looking at the fraud losses suffered by the banks and secondly, particularly when it comes to individual customers, are they treating their customers fairly? I have no direct remit to look at the way they are treating their commercial partners other than where it affects those two areas.

Q169 ***Baroness Hilton of Eggardon:*** Could you outline for me your powers and your role in relation to on-line banking services? Do you have sanctions that you can apply?
Mr Robinson: We have powers under the Financial Services and Markets Act. Under the financial crime objective we are given we are required to "reduce the extent to which it is possible for the firms we regulate [a bank or somebody else] to be used for a purpose connected with financial crime." That is broadly defined as fraud and dishonesty, market abuse and dealing with the proceeds of crime. We have a range of powers given to us under the Financial Services and Markets Act, ranging from civil administrative sanctions through to in some cases under the money-laundering regulations criminal prosecution powers, and indeed we have, under the insider dealer regulations.

Q170 ***Baroness Hilton of Eggardon:*** Presumably that is a last resort. I just wondered what your normal relationship is with on-line banking services? Do you have an on-going dialogue with them that keeps them in line or not?
Mr Robinson: We have an approach to banking supervision, most of the on-line supervision you are talking about originated from the banking sector, although I am sure not all, which is based around for a large bank a close and continuous relationship—that is not close in a cosy sense but very close monitoring at a high level. On a quarterly basis for example, you would see our supervisors discussing with the bank the latest trends, including fraud trends, that they are experiencing. That information is fed through our risk model and fed out to other supervisors so that we pick up the issues that are arising and feed them back in so that all of our supervision processes try to pick up on those risks. We very infrequently use our statutory enforcement powers despite the way it can often appear to people. We frequently, though, issue proposals to change behaviour in the form of a risk mitigation programme. As part of our risk mitigation assessment we will identify where Firm A seems to be doing less well than its peers, for example, or where its own systems have identified concerns, and will require them, through an audit letter, to change those issues which we will then follow up. We give them a follow-up point—it might be three months, it might be a year depending on what the issue is—and we will make sure that they deliver on that. Only if we find that an institution is failing to respond to those sorts of prompts do we move into the more invasive supervision processes which could involve a detailed review by our own expert financial crime review teams or the commissioning of an external report, the responses to both of which we would expect the firm to adopt, and if the firm is not doing that, or indeed has consistently failed to do what we require, we consider public enforcement action which has a proper appeal process and so on.

Q171 ***Baroness Hilton of Eggardon:*** In view of the rapidly rising amount of fraud that there seems to be in relation to on-line services do you think you are being sufficiently interventionist, sufficiently rapid in your response to the current situation?
Mr Robinson: I think it is the rate of growth that is very high. The absolute amounts of on-line fraud, for example, are not so great compared to the general level of fraud experienced in the sector. We are interested in the rate of growth and that rate of growth has meant that, for example, in the last two or three years in our financial risk outlook, a document we publish at the beginning of the year, we have alerted firms to the financial crime issues we have seen and our supervisory approaches have been driven by a wish to look at those issues and we are very active in following up concerns, so I would say that we believe that we have got a proportionate response to this but we are continuing to look very carefully from a risk perspective because the rate of growth is very high. Our starting point would be if the market is not delivering a solution then we should intervene.

Q172 ***Lord Young of Graffham:*** Mr Robinson, identity theft is apparently costing our economy an alarming £1.7 billion a year. Can you break that down in some way? How much of that is Internet related, how much of that is really people just impersonating others?
Mr Robinson: We can break that down a little bit. There is some information, I think, in our annex, but can I ask Mr Gruppetta to cover that particular point?
Mr Gruppetta: This particular figure, £1.7 billion, was put together by the Home Office as part of its work on the ID Fraud Steering Committee, of which we are a member, and the constituent organisations put forward figures for certain acts which they felt constituted ID theft. Due to the fact that some of those acts are quite different from each other it is quite difficult to break it down in terms of how much of that occurred on the Internet, I am afraid, but we

can, if you would like, provide you with the breakdown of each of the 16 members' figures.
Mr Robinson: Let me give you some illustrations to help understand the difficulty.

Q173 ***Lord Young of Graffham:*** Forgive me: I think the figures, if you could write to us, would be useful.
Mr Robinson: Certainly, we will do that.[2] May I add something about the difficulty? There is a combination of, for example, industry data that talks about estimating their financial losses due to ID fraud. There is information from the Home Office about the estimated cost to the Immigration Service of undertaking enforcement activity, and from the Passport Service, the cost to the Passport Service of measures to counter identity fraud, so it is a complete mix of information.

Q174 ***Lord Howie of Troon:*** We are told that there has been a rise in the rate of "phishing". Are you greatly concerned about this or do you see it as a minor issue in the general picture of financial fraud?
Mr Robinson: If I may I will make one or two preliminary comments and again ask Mr Gruppetta to deal with this one. As I have already said, the size of, for example, on-line fraud, banking fraud, customer not present fraud, is not very large in the quantum of fraud as a whole. However, the rate of growth is what concerns us. We have some things that we are going to do and I will ask Mr Gruppetta to speak about that.
Mr Gruppetta: As Philip said, we are very concerned about the rate of increase. I think it is about 8,000 per cent in the past two years, if you look at month-on-month figures.

Q175 ***Lord Howie of Troon:*** Very big?
Mr Gruppetta: Very big, but in terms of the actual size of the losses associated with that in the grand scheme of total fraud in the UK it is still quite small. However, we are concerned because obviously these phishing attacks are becoming more and more sophisticated. You do still see some quite primitive ones but they are becoming more sophisticated at the other end of the scale, so it is important that consumers do receive advice on how to stop phishing attacks and what measures and precautions they should take so that they do not fall victim to such attacks.

Q176 ***Lord Howie of Troon:*** You mentioned a very large percentage increase, quite staggering in its way. It is quite easy to get a big percentage increase from a low level. Is that part of the answer?
Mr Gruppetta: The figures we have, which come from APACs, and the actual figures I have got in front of me are different from the month-on-month ones that I referred to just now, but if we just take these as an example, from January to June 2005 there were 312 unique phishing incidents. In January to June, the same period for this year, 2006, there were 5,059 unique phishing incidents. We understand that that type of increase in the figures has continued throughout this year, so we were starting from a fairly low base in that there were 312 attacks. I suppose it depends how you define what is low, but it is much higher now.

Q177 ***Lord Howie of Troon:*** 8,000 per cent?
Mr Robinson: It does have some worrying aspects about it though. It is very easy to perpetrate these attacks in large volumes and so the consumer understanding of the issue and equipping consumers to know how to respond to what I think will continue to grow as a challenge is one of the key issues. Ninety-two per cent of the phishing targets seem to us to be in the financial service industry or connected to it, and indeed most personal financial data, whichever way it is acquired, will ultimately end up being used to defraud people in the financial system and therefore it is of interest to us wherever or however it is acquired.

Q178 ***Lord Howie of Troon:*** Could I ask you a question about banks? I gather that the bank marketing departments send out what you might call unsolicited emails and I am wondering if there were to be a general presumption that any unsolicited email supposed to come from a bank is fraudulent. The word is "supposed", of course.
Mr Robinson: My Lord, are you saying that the first presumption should be that marketing emails should not be responded to? It is probably a good presumption, actually, not necessarily because they are fraudulent.

Q179 ***Lord Howie of Troon:*** When people ring me up and say, "I have got a terrible opportunity for you", I have a great tendency to hesitate for a moment and just listen before I put the telephone down, because my presumption there is that this is fraudulent. Is that a sensible attitude on my part?
Mr Robinson: Regrettably, I think that not everybody takes the view that if it is too good to be true it is too good to be true, and not just in this area do we see these sorts of scams. I am sure we are all very familiar with the kind of 419 scams where people say you have won the lottery, give me some money. The earlier evidence session talked about the issue of marketing and how to separate from the plethora of marketing material that which is fraudulent and that which can simply be ignored and that which you might respond to because it may have advantage. I think this issue of

[2] http://www.identity-theft.org.uk/ID per cent20fraud per cent 20table.pdf

aligning marketing activities to incorporate thinking about managing fraud risk is something we have been talking to firms about over a number of years. Over the last two or three years, where we have started to talk to firms about how they manage their fraud risk in a more direct way, one of the things that comes up is the importance of every part of the institution thinking about how to prevent fraud in the way they are acting, and that means that when you are designing a product it makes sense to design a product that does not facilitate fraudulent behaviour. We are also doing that with institutions in the context of money laundering because that is another area of our remit. I do think it is a good question to ask if there are very large numbers of marketing material hitting your inbox, but how do you determine which are real and which are not when they all often look the same because the phisher or spammer has made it look just like it comes from your institution or an institution like yours. Typically, the phishing emails will impersonate a bank and they will send it willy-nilly to a name and address list or an email list that they have bought, possibly legitimately, on the Internet from people that market lists and they will send it out to anybody on the basis that if they send it to 10 million people some of those people might be banking with X bank and a small portion of those people that bank with X bank will respond to this email, and it is that small proportion that then get their money stolen. They may get 10 out of sending a million emails but that is enough. If you mix that issue up with the other things going out from banks it is very important. I noticed earlier on that there was reference to whether a website should identify itself. Reference was made by Visa to the secure system that is used increasingly by vendors. If the phishing issue becomes a really big problem in terms of the actual losses and those losses are not mitigated in any other way, then looking at some mechanism for identifying what is legitimate and what is not is going to be important.

Q180 ***Lord Howie of Troon:*** On the question of trust or trustworthiness do you think information of this sort which comes by way of email is less trustworthy than similar information that comes through the post in the old-fashioned way?
Mr Robinson: It may be, but I think that the volumes of this suggest that the numbers of fraudulent material that come to you is very likely to be higher because it is cheaper to send it. They do not have to pay for a stamp and so on, but I also think there is a problem with consumers being less wary on this channel. I said in a speech last week that the evidence seems to be that despite the fact that everyone has been warned about phishing, a small proportion of consumers, but it is only that small proportion who are ever at risk anyway, are prepared still to respond to this. Despite the fact that large numbers of people have been warned about it, and you talked about it being on the Internet and I have a leaflet here that was received by one of my children about fraud awareness from a bank that has lots of information about phishing and that happens mostly with all banks, but there is an issue of consumers listening, and I think there is a question of their perception of vulnerability on this channel which is rather an interesting contrast to the fact that they also seem to be fearful about it and I do not think we have clear data on this one.

Q181 ***Chairman:*** But do you not think we are at a point now when banks should not send any unsolicited emails to customers? You say phishing might be bad in terms of the total fraud sum that occurs, but phishing is a phenomenal problem if you are using a computer now. When we turn on our computers now 50 per cent of what we receive is this stuff. If banks send out no emails, and I think we have reached the point that banks should send out no emails, then we can start to put a lid on this because there would be a general awareness that people were never going to receive an unsolicited response from their bank, that anything to do with banking they will reject immediately.
Mr Robinson: My Lord Chairman, I have two responses to that if I may. I do not think it is correct to say in general (although it may be in your experience) that 50 per cent of the material on people's websites is phishing. Phishing is a very specific set of emails to collect personal data where they present themselves—
Chairman: I am talking about that combined with spam and unsolicited marketing.

Q182 ***Lord Harris of Haringey:*** Most of us get one a day, do we not? I certainly do.
Mr Robinson: There is a great deal of spam.
Chairman: There is a great deal of spam. If you only get one spam email a day you are in a very fortunate position.
Lord Harris of Haringey: No, there is a lot more spam. I mean one phishing email a day.
Earl of Erroll: I have some quite good filters so I do not receive them.
Baroness Hilton of Eggardon: I do not.
Chairman: I think we had better move on.

Q183 ***Lord O'Neill of Clackmannan:*** You have said several times, Mr Robinson, that consumer response is important. The difficulty is that consumers find it difficult to respond on a number of occasions. The obvious thing would be that if you had made a fairly substantial or what would be for the individual, an important financial transaction, would it not be desirable for them to be required to make personal contact with their financial institution either by

phone or by going into a branch? To do that you either have to have a call centre that can communicate easily with you or alternatively a branch which is relatively near at hand, let us say, within 24 hours, but the whole thrust of Internet banking has been the reduction of cost and in many respects the facility that is afforded to the consumer is a secondary consideration. Comment please.
Mr Robinson: I think that the move from the physical to the Internet channel or telephone banking in advance of that is driven by both customer satisfaction and cost factors. You mentioned earlier on that there is some sort of reward that arises because there is a higher interest rate often on these Internet savings accounts. We can see that consumers are interested in having the flexibility and the freedom that comes from being able to make payments and do things at different times on the Internet, and there are considerable benefits that flow to consumers from being able to do that but there are some security concerns that need to be put on the other side, so I do not think it is a clear statement to say it is second best. The other thing about large transactions is that what is a large transaction depends on the nature of the account. It is very much like we find in the money laundering area where you need to monitor the account for what is normal and abnormal. If I might give one example, this was a physical example and it could also happen electronically, I went to a shop to buy shoes and the person that put the amount the amount into the credit card machine pressed the double zero button too many times. I was not aware of this and as soon as this went in the telephone rang and it was the credit card company who asked to speak to me, was I there, yes, and told me that the shoes were going to cost me £6,000 instead of £60 or something, and I was very glad that they did. This response arises where there is an abnormal transaction, but obviously that was a very abnormal transaction. If consumers wanted to have this system of going into branches then I suspect the banks would provide it.

Q184 ***Lord O'Neill of Clackmannan:*** I take your point about the golden boot syndrome, but that tends to be a feature of credit card transactions, not banking transactions. I have found by travelling to other parts of the country or having a slightly different pattern of expenditure going to a shopping mall where I make purchases I have never done before, I have had that: I have been asked to verify certain things and I can never remember them and it is always very embarrassing, but it is reassuring. The point I am making is that the banks do not seem to be as rigorous as the credit card companies and there could be remedies to hand if there were a requirement on the customer—you have said consumer response, but I think there is sometimes a lack of consumer awareness that if they were entering into a transaction which was not common, that it would be to their advantage to contact the bank about it. I am not sure if you as a regulator can do very much about that but you can heighten awareness, but the complacency of the banks in these matters makes me very suspicious because they seem to think that because Internet banking is a bit cheaper, a bit more cost effective, it is a hit they can take. At the moment, of course, we are in the dark about this because they will not publish any information about this. We have had the trade association who, understandably, are merely the mouthpiece of the banks, but I think we may have to get the banks here themselves, just the big five, to justify it. Do you understand the frustration of some of us where we are really in the dark as to the size of the problem in terms of individual institutions and the like?
Mr Robinson: I understand that you are looking for transparency—

Q185 ***Lord O'Neill of Clackmannan:*** And accountability.
Mr Robinson:— about the size of the losses. Ultimately, of course, any losses are paid either by the shareholders or the customers, or perhaps both; it is a share out, so it is not a no-loss environment.

Q186 ***Lord O'Neill of Clackmannan:*** Too true.
Mr Robinson: Certainly the ability with which institutions manage their fraud losses is, if you like, a competitive element to that and one of the things that we have tried to do over the last three years is that if you think about it too competitively, in other words, "I am better than you; therefore I can have better margins or lower costs", you are playing into the hands of the criminal because what will happen is that the criminal will take their techniques and move into your institution rather than somebody else's or they will go from a bank to an insurance company to do similar things, and so what we have been trying to do over the last two or three years is to get the institutions to share information very rapidly, collect information, share it and also share information about good practice. The BBA, for example, publish a fraud managers' guide which brought together at a particular juncture their current experiences and they have these working groups that look at mitigating the risks. From my perspective as a regulator, making sure that firms have adequate systems of control to mitigate financial crime or fraud risk in this case, I can see these behaviours going on but I agree with you that they are not always transparent to everyone outside, but they are certainly happening.

Q187 ***Lord Harris of Haringey:*** One of your objectives is to maintain confidence in the financial system, and on 5 December Detective

Superintendent Russell Day of the Metropolitan Police was quoted as telling an all-party group of MPs that "banks were keeping quiet about attacks on their systems" largely because of concerns over public confidence, and you may remember the press were saying, "Are you saying that there is fraud taking place in financial institutions and they do not refer it on to the Met because they are afraid of it because it can damage them or because they do not think you can cope with it?" and they also replied yes. Do you agree that there is some evidence that there is a reticence by banks and financial institutions to come clean about the problems of fraud and about breaches in their own security because of this public confidence argument?
Mr Robinson: I think the banks are wary about feeding concerns by publishing information that will be misrepresented; I think that is correct. Certainly, when the officer answered yes about their concerns, he was asked a double question there in the quote that you gave, and the second part of it was about do they think that the Met will not do anything about it. It is correct that the likelihood of fraud reported to law enforcement being investigated is very low indeed.

Q188 ***Lord Harris of Haringey:*** I hope we can pursue that on a separate occasion as well. Are you saying therefore that there is fraud which takes place which is not reported simply because there is an assumption that it will not be dealt with properly?
Mr Robinson: That it will not be investigated, yes.

Q189 ***Lord Harris of Haringey:*** Earlier on, and I paraphrase the witnesses we heard, and you were here as well so you know what I am talking about, we asked about whether businesses should be legally obliged to notify customers and others of security breaches, and essentially we were told by the witnesses that really this would frighten the customers and so on. I actually found that quite frightening as a customer because what I was being told was they are going to keep to themselves the fact that my security has been breached in case I am more frightened. Do you think that is a way of maintaining confidence in the financial system?
Mr Robinson: I think that transparency about what has occurred is essential to maintain confidence. Our research at the end of 2005 looked at aspects of consumer confidence in the Internet banking channel and we will be repeating that. What it showed was, for example, a real concern that if the liability was moved from the banks to the customers they would move away from the Internet banking channel which showed the fragility in their confidence. Maintaining confidence in the financial system includes maintaining confidence in the transaction mechanisms in the system. I think that being open about what has happened is important. After all, it is the personal data of the individuals concerned. What was interesting was that no-one made reference to the Information Commissioner because this is personal data subject to the Data Protection Act and the Information Commissioner is the regulator for that area. One of the things that we are going to be investigating, and I might ask Mr Gruppetta to say other things about it, is how we should work with the Information Commissioner and with other regulators and entities that have personal financial data such as utility regulators and so on, because utility companies have this data for payment purposes, and some of the compromises we have been seeing have been personal data in the utility or telephone areas, which, of course, as I have said, gets used in the financial system. Understanding who has responsibility for making sure that the issues are dealt with correctly is something we are trying to do.
Mr Gruppetta: As Philip said, we have seen evidence that there have been security breaches in areas outside the financial services sector as well. I know there was a Channel Four programme, *Dispatches*, earlier this year which pointed to data compromises in particular institutions, and although this was banking data and, of course, the media reported this as banking data, it did actually come from other types of firms, particularly mobile phone companies were highlighted in that programme as being a fairly weak link. What we are trying to do is speak to other regulators of firms which hold banking data for payment purposes to see how we can work together and try and improve security right across the industry. As Philip said, part of this is going to involve myself and a colleague visiting the Information Commissioner and we are going to see him next Thursday just to talk about our respective responsibilities and what we might be able to do to mobilise some action in this area.

Q190 ***Lord Harris of Haringey:*** Would the FSA welcome clarity in the law requiring financial institutions to notify customers and others of security breaches?
Mr Robinson: The answer is that at this juncture I do not know whether I would welcome it or not. The reason I say that is that if the advice of law enforcement, for example, is that there should be no disclosure, and I have seen that happen in a number of cases because they are worried that that will compromise material further, I think it is very difficult to say that in every case there should be complete transparency. I realise that that is not necessarily in accordance, for example, with making sure that customers are aware that there has been a compromise, but I think there is a kind of tension of forces here because our presumption would be that making information available to customers is what

we would expect to see, but if law enforcement or others are saying that that will create an additional risk to fraud occurring, it is difficult to see that in every case you could make it a mandatory requirement. I think that is the sort of thing we need to look at with the Information Commissioner and others to see how that plays through, because the general presumption ought to be, and I think it is one we would have, that if information has been compromised that belongs to a customer and it could be helpful to them to know about it, and it does not create additional threat to them, they should know about it.

Q191 ***Lord Mitchell:*** This is on the subject of victims of on-line identify theft. How long and what cost on average does it take British victims of online identity theft to clear their names?
Mr Gruppetta: CIFAS, which is the UK's fraud prevention service, published some information on this fairly recently, and the information they published said that for a typical victim of identity theft in the UK, the main cost was time rather than money and it would take a typical victim between three and 48 hours of their own working time to put things right. However, if there was a total hijack of an individual's identity where perhaps 20 or 30 financial products or relationships with financial organisations were affected, you could be talking about a much greater amount of time, something around over 200 hours, I think they said. The cost of this in the report was about £8,000 where there was a total hijack. In reality we think a lot of that cost would probably be borne by the financial institutions involved, but obviously then, as Philip said earlier, it does affect probably the entire customer base or the shareholders of that firm, so it is wrong to say that nobody loses out in these instances.
Mr Robinson: Which is why, of course, the rate of growth in these things is what becomes important to us because a small number of these do not affect consumers very much at all but if a large number occurs it has a direct effect on consumer protection and on market confidence.

Q192 ***Lord Mitchell:*** In the United States victims are able to put locks on their credit records and everyone can have a free copy of their credit record once a year. Do you think we ought to introduce that here?
Mr Robinson: I think that access to credit information starts at a very low cost. It would be a market decision whether they wished to make that available for free. We certainly advise people on our own website, and indeed the ID Fraud Group on which we sat which produced this identity theft leaflet which was issued, part of that says that you should check your credit account and says that on average that could cost you around £2, and I realise that that is still £2 but it is not a very large a mount of money. The key question really is getting consumers into a behavioural pattern where they are doing the same online for identity risks as they do with their physical risks. Most people lock their house when they leave, most people lock their car when they leave their car, and I am afraid we are moving into a world where if you are going to use electronic banking it will not be the bank's branch that locks the door at night; it is going to have to be you locking it when you close your computer down.
Mr Gruppetta: If I could come back to the specific point about being able to lock your credit record, there is a facility available in the UK through CIFAS where, if a consumer believes that they might be at risk of identity theft or some data has been compromised, they can register for what is called protective registration at CIFAS. What CIFAS does then is put a marker against this individual so that if a financial product is taken out of that individual's name the banks will know that this is a higher risk application and they will look at it in more detail.

Q193 ***Lord Mitchell:*** Would it be in your view helpful, if there was a credit application made in someone's name, that that person should automatically be notified that that application had been made?
Mr Robinson: In general terms equipping people to understand what is happening in their name would be the sort of thing that we would support. It fits very closely with our financial capability agenda because that is about equipping people to understand the financial system better and information disclosure of what is going on is a very helpful way of alerting consumers. There is always a cost involved and again our general proposition would be that the market needs to look at what is demanded. It comes back to what consumers are demanding and whether or not if it is provided they will take advantage of it. We have just heard, and I think correctly, that unsolicited emails are often just ignored, so there is a real cultural aspect that needs to be sorted out. Personally I think that alerting people that something is being asked in their name, just like phoning up and saying, "This is £6,000 for a pair of shoes", is a very good way of helping consumers protect themselves.

Q194 ***Earl of Erroll:*** In the interests of bringing the online and offline world into alignment we heard earlier that the banks are now going to allow you to keep the money after a short period of time, in fact they said six days, even in a case of fraudulent transaction, so you have got certainty that the money is in your account. Should we be doing the same with online transactions because that only applies to cheques?

Mr Robinson: I think you heard what earlier witnesses said about the banking code's guidance. The only observation I would make in addition to that is that the electronic world is often a lot faster and some of the things that may be possible to do with the cheque clearing mechanism may not be possible in an online world but the banking code's commitment on repayment is—perhaps you can help me, Rob.
Mr Gruppetta: If a consumer has not acted negligently they will only be liable for the first £50 of fraud.
Earl of Erroll: And this will be on the online world as well as the offline.
Mr Robinson: That is already in the online world.

Q195 ***Chairman:*** Let me ask a final question. In the USA, they have recently banned US credit card companies and banks from making payments to online gambling companies. Many observers predict that this will bring alternative payment mechanisms such as "eGold" into the mainstream. Are you satisfied that such mechanisms are being properly regulated?
Mr Robinson: eGold is not regulated in the UK. It is available and used in the UK and it is not a UK regulated product. It is also used in a number of ways to make criminal payments, as has been said, on the paedophile sites and so on. What this demonstrates is the importance of the questions that were being asked earlier on about cross-border co-operation because the big difference between the electronic channel and the physical channel is that you have no idea where the other person is and it comes back to this question about the emails, where are they coming from? My advice to any consumer who started to move into any exotic exchange mechanism like eGold is that they should step very carefully in the way that one of your colleagues mentioned earlier on about what seems to be a good idea often turns out not to be. I can see no reason why there should be a large scale move to alternative payment systems like this for online payments. The issue is maintaining consumer confidence in the existing channels which are well regulated. This channel is not accepted, for example, by PayPal and other people like that for online payments and I think the message to consumers ought to be to keep out of areas which are not well regulated.

Q196 ***Lord Howie of Troon:*** Can you tell me what eGold is?
Mr Robinson: It is an interchange mechanism where you are exchanging amounts of virtual gold, the value of which goes up and down, rather than currency and the reason why it has been created in this way is to avoid some of the obligations that arise if you are doing it in money because if it is in money it will need to be regulated.
Chairman: Thank you very much. We have run on much longer than we thought we would but your answers have been very useful indeed to us. Thank you very much for coming to talk to us.

WEDNESDAY 10 JANUARY 2007

Present	Broers, L (Chairman)	Howie of Troon, L
	Erroll, E	Mitchell, L
	Harris of Haringey, L	O'Neill of Clackmannan, L
	Hilton of Eggardon, B	Sharp of Guildford, B

Examination of Witnesses

Witnesses: Mr Jim Gamble, Chief Executive, and Ms Sharon Girling, Team Leader and Law Enforcement Officer, Child Exploitation and On-line Protection Centre; and Mr Tim Wright, Head of Computer Crime, Home Office, examined.

Q197 ***Chairman:*** Welcome everybody, particularly our witnesses today. I would like to welcome Mr Wright back and Mr Gamble and Miss Girling, and welcome members of the public who are attending this session. There is a document available that describes this inquiry. I am Lord Broers and I am Chairman of the Committee. Everybody should note that we are being webcast today, just for your information. If we could start with our witnesses please introducing yourselves and then, if you wish, making a short statement. Shall we start with you Mr Wright?
Mr Wright: Good afternoon. My name is Tim Wright from the Computer Crime Team in the Home Office.
Mr Gamble: My name is Jim Gamble and I am the Chief Executive of the Child Exploitation and On-line Protection Centre and I am the Association of Chief Police Officers lead for countering child abuse on the Internet.
Ms Girling: I am Sharon Girling and I am a Law Enforcement Officer from SOCA and I work within CEOP.

Q198 ***Chairman:*** Would you like to make an opening statement?
Mr Wright: Just briefly. The Internet offers real educational and social benefits to children, as well as being a source of entertainment and helping develop skills they will need in the future. The Government is committed to ensuring that they can exploit those benefits safely. To do this, the Home Secretary set up in 2001 a Task Force to bring together Government, law enforcement, industry and child protection organisations to work on child protection on the Internet. That partnership approach has been effective over those years and in that time has delivered good practice for different companies that provide a variety of on-line services: chat; moderated chat; instant messaging; web-based services; and most recently social networking services. It has very nearly delivered a BSI kitemark for products to help parents manage how their children use the Internet. It has delivered training packages for police, prison, probation and social work professionals. It has delivered various public awareness campaigns aimed at parents and children to identify the risks and provide practical advice on how to manage them. The UK ISPs and the Internet Watch Foundation have effectively ended the hosting of websites containing illegal images of child abuse in the UK and the majority of the biggest broadband and 3G mobile network operators have put in place technical measures to stop UK customers accessing these websites when they are hosted abroad. Obviously the biggest development over those years has been the creation of CEOP which we will talk about. The Government set up CEOP to build on that partnership approach and to deliver a step change improvement in our operational capacity to protect children.
Mr Gamble: I do not wish to add anything just simply to associate myself with the comments that Mr Wright has already made.
Ms Girling: And I the same.

Q199 ***Chairman:*** We were told by the Government in November the importance of individuals taking personal responsibility for their own Internet security. Who is responsible for protecting children on the Internet?
Mr Wright: It is a shared responsibility in exactly the way as off-line safety is, and that underlines part of the partnership approach I mentioned. Obviously the Government has an overarching responsibility to provide a framework of legislation and agencies to ensure that everything possible is done. Law enforcement and the National Offender Management Service have a responsibility to reduce crime, to investigate offenders and to manage the risks those offenders pose in the community. Any company or individual providing a service to children has a responsibility to ensure that their children can use that service safely. Finally parents themselves and children have a responsibility to make sure they are safe. As professionals, I think we have a responsibility to help parents and children in this, through ensuring that on-line services have clear links to safety advice and how to report abuse but

also by raising awareness of the risks and providing practical advice. Over the last five years a number of organisations have delivered awareness and advice both to parents and to children. We have worked to ensure that these efforts are consistent and complementary as well as running our own campaigns. While the services that children use change over time, the three key underlying messages remain the same. Firstly it is more difficult to check out who you are talking to on-line than it is off-line and there are people out there who will exploit that. This is particularly important when children think about meeting on-line friends in the real world. Secondly, personal information you give out or a child gives out can then be used to contact them in a way later on that they cannot then control. And finally parents need to engage as much as they can in the way that their children use the Internet, both to understand what the children are doing, who they are talking to, but also so their child is more confident in turning to their parents if something goes wrong.

Q200 ***Chairman:*** That brings to mind the fact about parents themselves and who is responsible for educating parents. The evidence that we have had from the Children's Charities Coalition says that while a third of children regularly use blogs two-thirds of parents did not know what blogs were. Similarly almost 80 per cent of children use instant messaging but only a third of parents knew what instant messaging was. Given the rate of technological change can adults be expected to keep pace with the risks facing their children on-line?
Mr Wright: There are a number of questions in there. I think parents will always be behind their children because children are early adopters and tend to have more time to pick up new services. So parents will always be behind and older generations will always be behind their children. I think in terms of the detail of specific services and how kids use them—and certainly that research is consistent with everything else we have seen—the core safety message is that parents understand about safety and protecting their children, what they find difficult is applying that in the on-line environment. In terms of whose responsibility that is, it is a shared responsibility. Government, education, law enforcement, service providers all have a role in helping do that. It is an on-going battle for us.

Q201 ***Chairman:*** You do not think it would be valuable to have specific proposals that schools for example should run classes for parents, voluntarily of course?
Mr Wright: Some schools have tried but, anecdotally, take-up amongst parents has often been poor. I think it is a good idea, but from people I have talked to it is difficult to get parents to come into schools after hours and do it. Some parents will come and do it but they are the parents who already understand the issues. It is a good idea but we have not found a way of doing it successfully.
Mr Gamble: I think the issue here is demystifying some of the terms that we use about technology today. Tim is right, parents will understand a threat as it manifests itself to their children in the world that they grew up in and that they understood—the threat in the public place after dark. Talking about blogs sometimes is not helpful; talking about a diary, a parent understands that. So how do we engage them in a way that helps them develop a better understanding? We should be through our role encouraging them to be good parents in the sense that parents always were—to communicate with their children in a way to achieve better understanding. From the schools' point of view they need to imaginatively engage with technology so that the child's school report is delivered to the parent in the 70 per cent of homes that has on-line access in this country via e-mail as well as in the written form so that we are engaging them using the technology that we are speaking about in a positive and influential way. I happen to know that BECTA in the competition that they run to identify those schools making the best use of ITC, identified two schools who were joint winners and one was school was Ballyclare High School in Northern Ireland, and one of the questions that they asked the panel and one of the probing issues that they sought out was how they engaged with parents about the use of technology and how they used that technology to engage the parents. I think that is one of the ways that we see by being imaginative and engaging parents they are indoctrinated into the technology. The National Children's Homes' survey has shown that there is a massive gap between the knowledge that children have on-line and the knowledge that their parents have. We are never, ever going to be able to run technology classes to the degree that the parents can close that gap, but we can encourage them to understand it more effectively by simplifying it.

Q202 ***Chairman:*** You could almost get value, if these numbers are correct, by sending each parent half a sheet of A4 explaining what some of these things are.
Mr Gamble: Let me give you an example of one of the initiatives that we are running at the Child Exploitation and On-line Protection Centre. We recognise that we cannot police the Internet so as a serving police officer I recognise that the police cannot make all of our citizens safer on every corner of the information superhighway. Social services cannot, even industry by and of themselves with "safer by design" technologies cannot do that. We can no more be on every street corner in London than we can be on every street corner in the Internet. What

we can do however is identify those individuals who are at the greatest risk and we can empower them by engaging them in a way that delivers information that makes them safer. We are currently running an education campaign which is modern, it is contemporary media, using modern music and modern film in a way that engages young minds emotionally and intellectually, so that when the one million children we will engage by the end of this school term leave the classroom they will understand the nature of the threat. They will understand yes, go on-line, have fun, learn—those are the skills that are going to enable you to develop careers in the future—but they will also know where to go and when to report and, more importantly, what to report. Through that programme we are asking schools that when we engage with those children face-to-face that they are given a homework which involves sitting their parent down at the computer and saying, "This is what I have been asked to do today," and simply asking the parent to spend 10 minutes through the Think You Know education campaign by allowing their child to take them for a walk on the Internet and showing them that site. By simply doing that and by reviewing the top tips, a parent and a child will engage in a constructive conversation that will leave the parent better informed and the child reassured and perhaps given some more advice by the parent. I think that is the type of programme of work that we need to be involved in and we need to be influencing as many schools as possible to take it up.

Q203 ***Chairman:*** Do you think more can be done through regulation, for instance the Children's Charities Coalition argue for filtering products to be pre-installed on all computers and set to a high default security setting. What is the Government's view of the regulatory approach to these issues?
Mr Wright: The Government's approach is self-regulation where self-regulation is the best approach. In terms of filtering and safety products, we are close to finalising a BSI standard which will apply for these products to be accredited against because at the moment there are a lot of products out there and they vary in clarity and quality and parents are not well-equipped in choosing between them, so by having products that are accredited against a standard that parents understand, parents will be better able to choose between them. In terms of pre-installation, the next thing is to look at making sure that as many parents as possible are using them. Pre-installation is obviously one way of doing that and the Task Force is setting up a new group within that to look at how we drive the take-up of safety software, and pre-installation is one of the options on that.

Q204 ***Lord Mitchell:*** What is the view of manufacturers to that, are they co-operative?
Mr Wright: The manufacturers of the safety products have been very co-operative in developing the BSI standard. We have not got as far as talking to manufacturers and retailers of PCs about pre-installation yet, but understandably the people who provide these products have been very co-operative in developing this BSI standard.
Mr Gamble: The reality is that there is a commercial imperative in delivering software which is safer for families. People go and buy software on the basis of it being utilised positively by the whole family and the children in particular. So if you are someone that is selling something that people know is inherently safer then there is a benefit to doing that. In the Child Exploitation and On-line Protection Centre we partner very closely with industry and we have found that partnership to have massive benefits for us whereby we develop an ethical mutual interest in making children safer and we develop an ethical mutual benefit through that sharing of knowledge that allows us to inform them about where the risk manifests itself. Let me give you an example. Through the reports that we get into the Centre we are able to identify trends, themes and patterns. From that we are able to talk to manufacturers about where the threat perhaps manifests itself at any particular time. So that we know that Internet relay chat, instant messaging, is the environment where children are most likely to come into contact with a predator who wants to engage them. By working with one of our partners—Microsoft—very, very closely we were able to get them to sacrifice a space where they could advertise and gain a significant amount of revenue over a year to put our "report abuse" button in so that if you are a child in that environment and you are threatened by an inappropriate advance you are able to click on that button, initially get direct advice from us and then secondly report your suspicions. In the week that mechanism went on-line our reports went up 113 per cent. By working constructively with industry—we work very closely with Vodaphone, BT, AOL, Microsoft and others—we have found that we are able to gain a mutual benefit that I am not sure would be gained in the same way if we went for a regulatory approach. I have to say at this stage with my experience in the recent past, I do not support regulation per se.

Q205 ***Lord O'Neill of Clackmannan:*** Given that a lot of schools have pretty old computers and do not replace them very quickly, how confident are you that you can ensure that the software of the kind you have just been describing can be incorporated into school IT systems on a regular basis? Can you disseminate that information? Can you get it out? Are teachers able to load it onto the computers for the youngsters in their classrooms?

Mr Gamble: There are two different issues. The first is the stuff that can be bought commercially and we are working with the Home Secretary's Task Force and others to encourage manufacturers to meet certain standards so that people can be simply reassured and understand that that is safer. In the institutional environment, be it schools or care homes where many children are very vulnerable, we are working with some of the boards so that they better understand the nature of the threat. I know working with Vernon Coaker's office we are keen that by the end of 2007 at source many of the industry partners will have some form of blocking technology, and we are developing other initiatives which recognise that every provider will not be able to deliver that in the same way. In schools I can tell you this week the DfES have advertised for a grade seven member of their staff to work within our environment in CEOP so that they can engage with schools and ensure the safety messages that we are delivering and the guidance we are giving about what you should and should not do in schools goes direct to them. More importantly, I think in the longer term one of the key recommendations from this must be that this type of safety message is embedded in the national curriculum, and not just under information communication technology because it is about social responsibility. Let us not forget that technology is neutral. It is people who will abuse it or use it for positive means.

Q206 ***Baroness Sharp of Guildford:*** I wonder whether you could tell us a little bit more about CEOP since its inception in 2006. For example, precisely what is its role? What sort of resources are available to it? Are those resources adequate to the tasks that you face in this programme of trying to reach one million children with the message that you are trying to get over?

Mr Gamble: CEOP's primary aim is to identify, locate and safeguard children and thereby reduce the harm that they might otherwise face. It was built on the back of lobbying from groups not dissimilar to this one. It certainly represented the Home Secretary's Task Force, children's charities and the Police Service and industry itself. It was built to be different. We have constructed around three principal faculties. The first one is recognising that information in this area needs to be better managed and better shared, so the principal faculty is the intelligence faculty where we bring information in from police forces in this country and from abroad, from NGOs in this country and abroad, from industry partners in this country and abroad, and (since the launch of CEOP) directly from young people themselves. When we first launched we were getting about 21 per cent of the reports that came in from people below the age of 18. Today that number is up to over 40 per cent so bringing that information in, applying that analysis, identifying where a child might be at risk and identifying where an individual represents a risk to that child has resulted in national child protection operations where we have rescued eight children from contemporary hands-on abuse and arrested many, many more offenders. Bear in mind that academic studies will tell you that the average offender in the real world will offend against about 73 children, and I would say that is a conservative estimate, in the span of their offending career. The information, how we manage it and how we share it is critically important and are areas that we need to improve on. From that collection of information we create our second faculty which is our harm reduction faculty. Now that we better understand the nature of the offence, the nature of offender and the environments on-line and off-line where that is committed, it is about how do we create a "safer by design" technology, and we touched on that earlier. We have a safer by design team that works with industry and works with the Home Secretary's Task Force to encourage the sharing of information that can be translated into safer technology tomorrow, and we do that working very constructively with industry. That faculty deals with our education campaign. We could never reach one million children by ourselves so we cascade it out and we create and validate the product working with industry, working with charities and working with others. We make sure that it is contemporary and we have a youth panel presently of 60 young people made up of all of the diverse communities that represent the UK and we intend that to grow to 150. They come in and they advise us—does this touch you, does it grab you intellectually and emotionally in a way that would change your behaviour—so we listen to what young people say and we construct much of the stuff that we do on-line with their advice. That is situated in our harm reduction faculty. We have trained over 1,300 specialists in the UK from the Police Service, social services and charities around issues about understanding sex offenders on the Internet, interviewing sex offenders, and other training courses that we deliver. Our victim identification team is based in the harm reduction faculty. Those are the individuals that will take information from a police force, so seizing a computer in Manchester with thousands upon thousands of images and apply the lessons that we have learned in some of the operations that we were associated with earlier on to say how can we identify and locate and rescue the child. That is done by taking that information, applying an analysis on the clues that are available, and so far we have identified five children from that and we have 19 on-going investigations in that regard. That all sits in the harm reduction faculty with our academic team who work on a research

basis to help us better understand why people commit these offences and how we can interdict with them at an earlier stage to make a difference. The final faculty is our operations faculty and that is where we house our financial investigation team, supported by Visa International. We would be unable to deliver that on the basis of our core funding were it not for the significant financial and intellectual support that Visa International bring to the table. That is where we would target those individuals that operate in a pay-per-view environment treating child abuse images as a commodity. We now attack them in the same way we would have before a drug dealer who uses cocaine or heroin as a commodity. We also use that specialist resource to identify patterns of life. If you are a sex offender, where are you going, what are you buying, what are your intentions about travelling? So we build that picture up and it helps our offender management team help the multi-agency public protection panels when they look at the most high-risk offenders. We have a second team which is our covert Internet investigations. They at this moment in time are engaged with counterparts across the world—Canada, America, Australia, Italy, with Interpol—where we are engaged in infiltrating those paedophile groups in the real world who use and abuse the technology to share information with one another to minimise and self-justify the behaviours that they enact, and to help identify, interact with and locate children they can reach in the real world. So that group is infiltrating as we speak and you will see over the months that follow the results are going to be outstanding and the evidence will be available in the public arena in the not-too-distant future. Finally we have an operations support team there that go out to forces providing forensic behaviour analysis support and also providing co-ordination support in this country and abroad where we are able to raise levels of awareness. After all I have said you probably think I am going to say we have got several thousand people. The Centre is about being more intelligent as opposed to being simply larger. There are between 80 and 100 people currently working in the Centre from a variety of backgrounds including the Police Service, the Serious Organised Crime Agency. The NSPCC has embedded a significant number of its personnel in our premises. Microsoft has embedded a significant number of their personnel working for us within our premises. Different government departments are represented within the premises so it is a partnership that manifests itself in reality every day across a desk and not at a meeting you might or might not attend once a month. Hopefully I have not gone on too long and that has given you a feel.

Q207 ***Baroness Sharp of Guildford:*** In terms of resources, which was of course one of the questions I asked, I take it from what you say that it is a mix of public and to some extent private sector resources that you are getting? You were talking about Visa but you are also getting resources in from Microsoft and some of the children's charities.

Mr Gamble: That is correct and we could not operate without that support from industry, from the children's charities, and from others.

Q208 ***Baroness Hilton of Eggardon:*** Carrying on from that, clearly a lot of your work is reactive to information that you receive. To what extent are you able to be proactive and go out looking for paedophiles for example or other people who may be pursuing children and grooming them?

Mr Gamble: Through our partnership with the Virtual Global Task Force, which is a collaboration of international law enforcement agencies which I chair, we operate 24/7 on-line on the Internet. That is undercover officers from Canada, America, Australia and the UK, shortly to be joined by a new partner I hope in Italy, sharing the patrolling time that we need where we will visit the locations where intelligence indicates to us that people are gathering that represent a threat to children so we engage them. That is low cost and high impact. What it means is that whilst we are working the Canadians are sleeping, they then take on the next shift, the Australians the one after, and we have the overlap with the Americans. It means as well that we are able to engage paedophile networks in a much more holistic way than we ever could before and we can call on resources to reinforce our activity that are not simply within our own jurisdiction because where we are proactive—and we are very proactive at present—we do that on the basis of attacking the threat, not on the basis of the geography of where it manifests itself. You cannot do that on the Internet. You have to sacrifice a little bit of your own sovereign territorial responsibility. What people need to understand is as child if I am a 15-year-old girl who exposes myself on a web camera to someone I believe is a 16-year-old boy, the offence has taken place and that image will be forever shared and as a 47-year-old paedophile I will use that image when I am engaging a 15-year-old boy to pretend that I am a 15-year-old girl and I will share that image pretending that it is me. So the perpetrator in that regard can be in Canada, America, Russia or Australia and can capture that image and that child is revictimised every time that image is shared or sold or swapped. We are looking in that regard at the value of an image, so when we capture someone who has a huge collection we can quantify what does that mean in a financial sense and can we use the Proceeds of Crime Act to remove the benefit that they have accrued from them and to make an investment in child safety in the future using those ill-gotten gains.

Q209 ***Baroness Hilton of Eggardon:*** What other organisations do you liaise with, the Internet Watch Foundation for example?
Mr Gamble: We work very, very closely with the Internet Watch Foundation here in the UK, and with charities large and small. We met with Barnado's yesterday about post-incident trauma counselling for children. We work with every government department, very closely with BECTA, very closely with DfES, very closely to the National Offender Management Team and all of the charities that you would imagine, headteachers' associations, the Football Association, anywhere where children will go we are able to engage and influence them. If you were to visit the CEOP centre, which I would really encourage all the Members to do, and test the DNA when you were there, the DNA would reveal partnership. There is nothing that we do that we do by ourselves. It is about this mixed ingredient that builds something which is significantly different, and the results that we have had to date evidence the fact that the proof of the concept that we have delivered in this first year needs to be significantly reinforced in the years to follow so that we can capitalise on the early success.

Q210 ***Lord Harris of Haringey:*** I want to pursue the question of whether there are adequate resources available working in the area of on-line child protection? Are there sufficient police officers? Are there enough police officers with the appropriate training? Is there enough appropriate equipment in the Police Service? Are there enough other staff, other agencies? Could you give us some indication of that?
Mr Gamble: First of all, let me say about the Police Service, do we need more police officers to be engaged in this work? Yes we do. Do they need to be in our building for example? No, they do not. Are the police of themselves necessarily the right people? What we need is more people with the right skills. Some of them will be police officers, others will be members of industry, others will come from social services with a particular understanding about the impact of harm on children, and some of them will be from government. We do need more resources. We do not need massively large amounts or significant amounts of reinforcement. What we need is the right people in the right place and a more intelligent approach to co-ordinating our activity. The benefit the criminal sees in the Internet is that they can be in many places at many times representing themselves in many different guises as different people. We can turn that against them. A small group of highly trained covert investigators can be many people in many places targeting many criminal entities, and we need to make sure that we get the best use of UK resources by more effectively focusing what we do around a tasking and co-ordination process, and we in ACPO are currently working on just that thing through our Countering Child Abuse on the Internet Group.

Q211 ***Lord Harris of Haringey:*** Operation Ore led to something like nearly 1,500 convictions in the UK yet I have also been told that it could have been a lot more but there was a resource constraint. What impact did Operation Ore have on police resources and on the wider criminal justice system at the time and what were the pinch points?
Mr Gamble: I think there is a lot of misinformation about Operation Ore and I welcome the opportunity to address some of those issues now. Operation Ore was a wake-up call. Operation Ore and the seeds for it were planted in the late 1990s when a couple in America who sold pornographic images to customers through acting as a web conduit found out quite by accident that they could make significantly larger amounts of money by selling abusive images of children, so they are organised criminals who are good business people because they divert to an area where they see the risks being lower and the profits being higher. We were not prepared for that in UK policing. I do not think social services, I do not think any of the institutions, even the academic ones, would ever have foreseen the fact that we were going to be hit with that number of suspects. Let us be clear, did we learn lessons in Operation Ore as a service? Of course we did. I think it is important to recognise that the volumes were unlike anything anyone had seen before in a single crime type and it was complex. Sometimes people were seduced by the complex nature of it because it is the Internet and you see it as a labyrinth and where do you go. I think historically there has been a tendency to say, "We cannot do anything about it because it is the Internet. We cannot make a difference because this technology is something we cannot understand." The principal lesson we learned from Operation Ore is this: the Internet is simply another public place, it is like this room, and the Internet is not good or bad; the people who occupy it at any given time will decide how good or bad it is. From a UK policing point of view, the lesson we learned is when you look at the suspects in these cases you have to categorise and prioritise them on the basis of those who represent the greatest potential risk to children. We did that and to date there are over 2,300 cases that have been dealt with through the judicial process and there has been a finding of guilt either through conviction in court or in just over 600 cases cautions. Police cautions are not given out on the basis of it being an easier route to reconcile and draw a line under a case. Police cautions are given out under national guidelines where there is a realistic likelihood of conviction and where the individual concerned has made a full and frank admission in the full understanding of the consequence of that. Anyone that accepts a caution

for a criminal offence is guilty of that offence. Make no mistake about that. It is the same as if I am convicted today and say, "Actually I am innocent, I only pled guilty because I wanted to get it over in time to go and do something else or to move on beyond it." Anyone who has had a caution administered is guilty. Operation Ore represents a success. Let us be very clear, 132 children were rescued from actual live time abuse. That is a success. The police however began to view it in a different way: should we in the future be focused simply on finding where images are? I do not think so. We need to adopt a different approach. It is people that put the images on the Internet, it is not the technology. We need to be focused on the people who create the harm by taking the images in the first place because every image represents a victim. Every child is a victim in the first instance and revictimised in the second instance. I think Operation Ore was great work by the British Police Service and I would want to give them credit where credit is due for that and dealing with a difficult and complex area of a new crime type or an old crime committed in a new environment whereby they were able to do something that rescued that number of children.

Q212 ***Lord Harris of Haringey:*** Could I stop you there. Certainly I was not trying to criticise the work you have done on Operation Ore; it is a question of whether more could be done. If it happened again with a similar sort of situation, could you take us through a little bit who takes the lead on this? Is it yourselves, is it SOCA, and I know SOCA has been criticised for allegedly downgrading its response to Internet crime, or is it the individual police forces? How is that responsibility allocated?
Mr Gamble: The national responsibility as a single point of contact would be the Child Exploitation and On-line Protection Centre. The lessons that we have learned in dealing with Operation Ore have meant that it will be processed in a much more effective and efficient way. We learned lessons when we began to deal with what was an old crime committed in a new way previously, so that would come to us now. We have the mechanism and the infrastructure now to allow initial assessment of the intelligence and intelligence development to happen in a processed way. If you were able to visit I would be able to show you how that works, where we take the intelligence in, we establish whether there is a potential live time threat to a child and process it as a priority. Where there is not that immediate evidence, that information is then developed to a degree that we can decide whether or not a person has committed an offence. Let me give you one quick example. I mentioned to you that we are working on pay-per-view sites. We looked at a pay-per-view site facilitated in the UK. We were able to operate to a degree using undercover officers as well as financial investigation so that we were able to test the evidence prior to making arrests. Without going into the detail of cases that are still in court, I can say that in those cases the full and frank admissions that were made immediately evidenced to me as a serving police officer that that is an improved process, an improved way forward. We would not have got there without experiencing Operation Ore. Also it is worthy of note that in many, many cases where we have investigated, and we are duty bound to investigate them all, we have taken no further action where there is a doubt. We have given the benefit of that doubt to the suspect, as is right.

Q213 ***Lord Howie of Troon:*** You have partially answered my question which was, was this a new crime or an old crime using a new medium?
Mr Gamble: This question is asked a lot—one of the interesting issues, and I do not want to waste your time, is that in 1874 a local photographer in the Pimlico area, Henry Hayler, had over 130,000 photographic images seized held on 5,000 glass plates. Those pornographic images included images of him, his wife and his children, so it is a crime which has been with us I think always. It is a crime that the Internet allows those who are motivated to do so to exploit to a different level and to a different degree, but the good thing is this guy Henry Hayler left the jurisdiction and we believe he either went to Berlin or New York where he continued to share images for some time and in today's world the forensic contact with the on-line environment would give us many, many clues to track him. The relationships that we have through the Virtual Global Task Force, through our participation in G8, and through our partnership with Europol and Interpol would mean the likelihood of him remaining at large until he wrote his journal and subsequently died would be strictly limited.

Q214 ***Lord Howie of Troon:*** If it is an old crime in a new way, do you need new laws or can you catch the perpetrators using the laws which exist?
Mr Gamble: In most instances we can use the laws that currently exist. If you take the public place analogy, people will go to and frequent a public place, sometimes on payment or otherwise, but it remains in essence a public place, and the common law and the precedent that has been set over the years is something that we should not easily move away from. Where we have needed law that is more flexible and that understands the technology, such as grooming and the sexual offences legislation, then we have found Government and others very willing to be flexible and to look at that in a different way. Through the Home Secretary's Task Force a particular subgroup continues to look at that and we

are considering cartoon images, for example. In the future we are going to have to look at the written word and the harm that can be conveyed by an obscene publication in that way in the on-line environment. You might want to consider for example as a question, is it right that as a 47-year-old man I can go onto the Internet tonight and pose as a 14-year-old to talk to a girl who is 13? Forget about sexual intent, is it right that I should be able to do that? Why would any 47-year-old man ever want to engage with a 13-year-old girl whilst masquerading as a 14-year-old boy. I think without lawful authority or reason you should not be allowed to do that. So do we need to look at other aspects of the law? Yes we do. Have we found the system to be willing to consider and contemplate how those could be developed? Yes we have.

Q215 ***Lord Howie of Troon:*** Have you any proposals for new laws?
Mr Gamble: I have a number of proposals that I would like to make before the end but none of them relate to new laws. To be fair, it is not about new legislation. It has got to be about new thinking in this environment and that is what we have found to be far more effective.
Mr Wright: We have been very keen to review the law and see whether it is fit for purpose. Just to clarify what Jim said, the Home Secretary is currently consulting Cabinet colleagues about whether to ban the possession of computer-generated images of child abuse, including cartoons and other graphic illustrations of children being abused.

Q216 ***Lord Howie of Troon:*** So possession rather like possessing cannabis?
Mr Wright: Yes and at the moment the possession of real images is illegal but the possession of computer-generated images is not illegal.

Q217 ***Lord Howie of Troon:*** Is that really because e-crime is scarcely recognised?
Mr Wright: I think it is because the original legislation was about protecting children and an image of a child being abused is directly related to protecting that child because the child is harmed and abused in the creating of the image. In computer-generated images it is rare for a child to be harmed in the creation of the image so the legislation grew up differently but now we think we should ban the possession of those as well.

Q218 ***Lord Howie of Troon:*** Could you give me some notion of the size of the problem? Is on-line child abuse getting worse or increasing? You mentioned something like 132 children. I do not wish to disparage your work but that is not terribly many children.
Mr Gamble: But that is Operation Ore and if you look at the number of individuals arrested and acknowledge the fact that over their lifetime of offending academic evidence would indicate to us that they offend against many children. Let us look at a recent case. Lee Costi was convicted in Nottingham last year, a young man who had gone on-line and habitually engaged with 13 and 14-year-old girls and whose method of operating was to engage them on the Internet and then to meet them at a train station where he would engage in sexual activity with them. If you look at the computer hard drive and you examine it, you will see that he had conversations with many, many, many young people all of which, given the right circumstances at the right time, could have led to offending, so the preventative technology here is important. Secondly, people sometimes become confused by saying you are misdirecting child protection activity here because the real harm takes place in the home or in the broader family circle. They need to recognise the fact that a computer (which is in 70 per cent of homes which gives on-line access) allows children to form intimate relationships in the way they once only did with close family and friends living in the proximity. So is it a problem that is growing? I do not think it is. Is the profile of it growing because people are becoming more aware? I think that is the case. Our job is more about child protection however than about technology and one of our great fears is that sometimes we become so seduced by the technology in these issues that we lose sight of the issue which is protecting children no matter which environment they happen to be in at any given time.

Q219 ***Earl of Erroll:*** I was going to ask about whether the existing laws were adequate for dealing with people acting illegally on-line dealing with people accessing illegal on-line content but I think you have really answered that. One of the things that concerns me is that some of the evidence of some of the stuff that is going on can be discredited if you start accidentally bringing innocent people into the net, and it was said that there were a certain number of people whose credit card details were held by Landslide Productions (which led to Operation Ore) where there was no evidence they had accessed any illegal content and yet they were in some cases apparently hounded. There was also I heard word that some of the images that were found on computers may have only been sitting in temporary Internet files because they were hidden behind thumbnails on the front page and people had not actually gone into that part of the website. Do you have any comment on that?
Mr Gamble: In order to access the Landslide website there was a process that you had to go through. Let me say for the record I am speaking generally now

because it would be inappropriate when there are still some cases pending for me to go into detail. The principal operation of Landslide was simply this: you went on; you identified what you wanted; you handed over your credit card details and you were sent a password back to your e-mail address which you had; you then went back on-line using that password which had been sent to your computer and then accessed your chosen choice. People have said, "Well, it said here 'click child porn', and it did not." In some cases of course it did not; in some cases it said "click here for child rape". Where those people have been investigated, they have been investigated first and foremost because there is a reasonable ground to suspect that they may have committed a crime. They are not guilty in the first instance. That case came to what was then a paedophile investigation team and went out to an individual police force. The individual police force independently assessed the evidence and independently investigated it. At the end of that independent investigation that information, including the process by which they accessed the site allegedly, went to the Crown Prosecution Service which independently assessed the veracity of the information placed before them and whether or not there would be a likelihood of prosecution. Once they had made their decision it went to the court system where a judge made a decision independently about the veracity of the evidence produced by the prosecution and the information provided by the defence. It is common practice in many cases—and I have been a law enforcement officer for over 26 years—to try and discredit an operation of any type, not least this type in a new area. I would not want to associate myself with any investigation that manifested itself in the way you described, and that does not bear any resemblance, in my view, to my actual experience of this investigation.

Q220 ***Earl of Erroll:*** Can I just say this was not an attack on the police or the police involved or you yourself at all. It is perfectly possible, given the technology involved and the complexity of the way some things would be accessed, that mistakes can be made, particularly as this was a new area for many of the investigating police so therefore it is quite possible that these things could have happened. A very quick question then, there was no other sort of pornography on that website, it is purely child pornography? I have never visited it so I do not know.

Mr Gamble: I am glad because we would have met under other circumstances perhaps! Let me be very clear here. Without going into too much technical detail, which I think would be unhelpful, was there ever a doubt about a particular aspect of a particular part of Landslide? Yes. Were they ever pursued or prosecuted? No. So where we identified in that investigation a doubt we then took action to make sure that those individuals were removed from that cloud of suspicion. The difficulty here is we understand, and we understood at the time, you cannot make this allegation and then withdraw it easily and put somebody's life back together. We understand that and that is why there is a lot of due diligence and that is why it takes a lot of time.

Q221 ***Earl of Erroll:*** Is there possibly going to be a problem with the amount of credit card theft—identity theft as people have re-named it—that is going on at the moment? Is that going to be an increasing problem in future investigations firstly making sure that the credit card details were not stolen?

Mr Gamble: We never prosecute someone simply on the basis of their credit card being used. You are going to look at all of the circumstantial evidence which when taken together provides overwhelming evidence. No, I do not think so and I also think that the pay-per-view industry is moving away from the simple credit card transaction. We are looking at other mechanisms whereby they can hide the activity they are involved in. So I do not think that that will be a problem in the future.

Q222 ***Lord Mitchell:*** I was interested in your view on the emerging threats to child safety, for instance as a result of the extension of connectivity to an ever-wider range of devices. By that I am sure we mean mobile phones, wi-fi connected iPods, devices like that.

Mr Gamble: It does not matter what the technology is. We need to move away from looking at the apparatus that actually delivers it, whether it is the mobile phone that is the brick or the new one that you can listen to your music on and also get onto the Internet and check the football scores with. What this is about is the threat that will emerge which is one of ignorance and perhaps arrogance on behalf of the Police Service and others in positions of responsibility where we assume that we have done enough and where we assume that children know enough. I go back to what I said before, I believe the best way of dealing with the emerging threat is through education. It is through engaging with children and actually listening to them. The youth panel work that we are doing, listening to academia, listening to young people about the way they occupy this new space and capitalise upon it in a way that helps them identify what the risks are and helps them contribute to the solution. 30 per cent of the reports we receive in the Centre are not about the technologies themselves and are not about something that industry creates; they are actually about the way children behave in that particular environment where

they are given scope. It is about some of the self-generated content that they will share with others, and that is about education. That is about what you talked about earlier, talking to parents. A parent may not understand what a social networking site is. A social networking site is a fantastic place for young people to keep in touch when they go to university with their friends at home and elsewhere. Some criminal element will try and take advantage of it. I ask you this and I say this to parents: would you allow your child to wear a billboard or sandwich board, or whatever you want to call it, with their home telephone number, all of their personal details on it, and some handout photographs that they would walk from Victoria Station down to Oxford Street with whilst every Tom, Dick and Harry in the street could see them? You would not. That is about educating people and simplifying and demystifying the aspects of technology that we tend to lean towards in these debates.

Q223 ***Lord O'Neill of Clackmannan:*** You mention that because of international co-operation you can now have 24/7 sharing of a lot of the monitoring. How much further do you think you need to go in this area of international co-operation?
Mr Gamble: We need to build on the Virtual Global Task Force partnership because one of the questions about the numbers involved means that the long arm is able to be that much longer. I can say, without divulging too much, that we are currently investigating hundreds of suspects in on-line environments at present who are trying to access children because of that partnership. I believe Italy will be full members within a short period of time. We are working through the G8 initiative and those infrastructures that are already available to see how we can expand. The key in the next phase of development is going to be engaging countries that are not as technologically advanced as we and some of our partners are and recognising that what we see here are symptoms of crimes, and the root cause sometimes in their jurisdictions, and we need to support them build an infrastructure that means they can play a full part.

Q224 ***Lord O'Neill of Clackmannan:*** Are you getting the co-operation from all of the countries that are as technically advanced as we are? Are other countries within, say, the EU that have fairly sophisticated IT environments all playing their part or are there still some people who perhaps are not as conscious of the nature of the problem?
Mr Gamble: I think there are some places that are not as conscious but everybody plays a part in protecting their own children. I have been involved in my career in many types of crime ranging from terrorism to organised criminality and I have not been involved in any area where you get such a degree of enthusiasm and willingness by agencies, voluntary and government, in jurisdictions because protecting children is something that everybody can relate to. We do need to get better at it and some individual states need to recognise that they cannot protect their own children within their own geographic boundaries. The partnership needs to rise above that.

Q225 ***Lord O'Neill of Clackmannan:*** If you think about it, the creation of CEOP is in itself a recognition that this is a particular type of crime, but is there still a danger or are we still in the position where this form of crime is seen as part of the general e-crime agenda?
Mr Gamble: I think there is a danger that it is seen as part of that and we would not want it to be perceived as such. I think the label e-crime is unhelpful. E-crime should relate to those new crimes which are truly facilitated by the technology—the phishing and those types of attacks that you will see perhaps. From my point of view, and I was previously the Deputy Director-General of the National Crime Squad and I have some experience with the build of the National High-Tech Crime Centre, the Child Exploitation and On-line Protection Centre is about protecting children, it is not about the technology. The technology assists us and we use it to positive effect but I would not want the work that we do to be seen as e-crime.

Q226 ***Lord O'Neill of Clackmannan:*** In the international context does that position prevail as well? What you said holds good for the UK but is it the case across the forces with whom you are in most close contact?
Mr Gamble: No, it is not the case. In some areas I think they are moving to that more holistic approach. We have had visits from other jurisdictions from some other parliaments to look at the UK experiment with CEOP and that has been extremely positive. Our colleagues in America through the National Center for Missing and Exploited Children again are focusing on the child aspect and bringing technology to bear as a constructive tool, but no, it is not recognised, and one of the problems with technology is everybody always defaults to it. The technology itself is not relevant. It is like trying to place a certain crime in a particular geography. It is about how we capitalise on the techniques that allow us to protect our children because very often technology will be used to lure a child from the virtual world into the real world and if you divide the way you deal with that then you undermine the activity.

Q227 ***Lord Howie of Troon:*** You mentioned the United States a moment ago. We are told that more than half of child abuse image websites are hosted in

the United States. What is being done about that over there?
Mr Wright: I think it is fair to say that despite best efforts and the sophisticated tracing techniques used by the IWF it is not always possible to be categoric about where a site is hosted. A lot of websites, particularly the commercial ones, move frequently between jurisdictions as part of their efforts to avoid disruption or detection. This is a subject that the UK Government and agencies continue to raise with other governments, including the US, for example, through the G8 where justice and home affairs ministers gave a commitment to redoubling our efforts to combat the availability of these images. It is always difficult to judge other countries' approaches but the US Government over the last few years is attaching increasing priority to this issue. Nearly a year ago it launched its Project Safe Childhood to enhanced its national response to "combat the proliferation of technology-facilitated sexual exploitation crimes against children". The project brings together federal resources, NGOs, and state and local law enforcement through a national network of Internet Crimes Against Children Task Forces with additional federal funding. The project includes integrated federal, state, and local efforts to investigate against individual people exploiting children, better community awareness, better education and better training for law enforcement and has led to every law enforcement agency developing significant operation initiatives against child exploitation. The US House of Representatives' Committee on Energy and Commerce conducted recently a hearing on "Making the Internet safe for kids: the role of ISPs and social networking sites", which has looked in detail at the hosting of images in the US and taken evidence from ISPs and NCMEC about this issue. Additionally, the National Center for Missing and Exploited Children has begun sharing the signatures of known child protection images with ISPs so those ISPs can start to eliminate the individual images from their systems. In summary, a lot of images are still hosted in the US but we are starting to see from the US Government a different and a much stronger approach to attacking it.

Q228 ***Lord Howie of Troon:*** Our Government presumably is encouraging the United States to deal with this?
Mr Wright: Absolutely. I have seen it on a number of occasions. It is diplomacy and you can only encourage but we have been encouraging them for longer than I have been in this job and we are starting to see action on the ground.

Q229 ***Lord Howie of Troon:*** How long have you been in the job?
Mr Wright: I have been in this job for nearly five years.

Q230 ***Lord Howie of Troon:*** Are there any other blackspots apart from the United States?
Mr Wright: In terms of hosting of images, it moves around quite a lot. Russia sometimes and increasingly Japan and Spain now are part of the problem, but I think there is a danger in focusing too much on in which country the server is where the images are because it is trivial to host any form of website in any country around the world, and moving it is $30 and half an hour's work. These sites will always be moved to the places where they think it is the safest for them, where the ISPs will provide less information to law enforcement, so even if all four countries identified changed overnight, in terms of people accessing the images there would be no disruption because the images will all be hosted in four different countries. I think it is about building co-operation globally, it is about attacking the people behind the images, the companies putting the images up, and most people are not based in the countries in which the website is hosted. The other thing which we have done in the UK very strongly is looking with the ISPs at blocking access to images wherever in the world an image is hosted. The majority of large UK ISPs will now block access to images wherever they are hosted because while we have pretty much eradicated the hosting of these websites within the UK they were still as accessible to UK residents as they were before, so what the UK ISPs have done is said, "You tell us where these images are and we will block access to those images wherever in the world they are," so even if those four countries cleaned up their act and it is four different countries next week, people in the UK will find it harder to access those websites.

Q231 ***Lord Howie of Troon:*** In records, does the style and taste of the images depend on the country from which they come?
Mr Wright: No. I do not think there is a difference between the country from which the image comes and the country where it is hosted, but colleagues have more knowledge about the images.
Mr Gamble: Let us be clear, to adopt a position whereby we were to suggest that the United States was in some way well behind everyone else would be fundamentally unfair. The vast majority of the Internet infrastructure is based in the US, so the key word here is that a majority of those sites will "appear" to be hosted in the US, and I think technically we need to be very careful what we say there, they will appear to be hosted in the US. Images will be the same. They will be horrific and that is why we in the UK are very positive about not using the term "child pornography". We do not believe that

what we are talking about is child pornography. Pornography is something which, depending upon your moralistic view, may be legal or not. This is not about consenting adults performing an act for the gratification of a third party on payment. This is about children as young as weeks old, sometimes unfortunately even younger than that, up to their early teens where they are physically abused in the most horrible sense by adult males. One of the things I find most disturbing, and we see a lot of images to put this in context, is a young teenage girl in a video we currently are working on who talks as if she is a 40-year-old prostitute. That child has been so badly treated and so heavily indoctrinated into the darker side of producing these types of images that she now behaves in a way that you would imagine if you were looking at it for the first time, that she was somehow complicit, but she has been victimised over so many years. The US in many senses has led the field in some of the initiatives it has brought together, partnering with industry. When we built the Child Exploitation and On-Line Protection Centre, we looked at the model of the National Centre of Missing Exploited Children to see how they did what they did and how we could apply the best parts of that here in the UK. They are active partners, they are members of the Virtual Global Task Force. On Monday of next week, an agent from the Department of Homeland Security will begin in the Child Exploitation and On-Line Protection Centre here, a physical manifestation of that partnership. We work in close partnership with them and we are able to use the technology to make that partnership a day-to-day exchange of information.

Q232 ***Lord O'Neill of Clackmannan:*** You mentioned what you thought would be desirable in incorporating Internet safety in the National Curriculum. The impression I got was, therefore, that it seems a somewhat patchy process at the moment. Is Internet safety covered in the school curriculum in any organised way and at what age do the signals start being sent, the warnings?
Mr Wright: There is flexibility in the ICT programme of study to include teaching about Internet safety to pupils. Schools are encouraged to integrate e-safety messages across the curriculum and implement policies and safe practices on Internet use, and teachers are provided with the resources to reinforce responsible use of the Internet. The Qualifications and Curriculum Authority have adapted ICT schemes of work and guidance to strengthen the message about Internet safety. DfES have worked with the QCA and Becta on developing resources and guidance for schools, for example, under the Internet Proficiency Scheme, and the 'Signposts to Safety' publication provides advice on teaching Internet safety at Key Stage 3, which is 11- to 14-year-olds and Key Stage 4, which is 14- to 19-year-olds. The scheme is a specific way of developing safe and discriminating behaviours when using the Internet.

Q233 ***Lord O'Neill of Clackmannan:*** So it does not start until the age of 11?
Mr Wright: It can be taught earlier. It can be fitted into the curriculum there, but I do not think that it is taught at every school.

Q234 ***Lord O'Neill of Clackmannan:*** At the moment you are saying it is taught through the medium of the subject ICT and it is not taught as children are learning to use computers, as they are, at primary school? It does not seem to be happening there. It may well be happening, but it is not happening in any organised way. Is that right?
Mr Wright: It is taught as part of ICT, but it is up to individual schools and it is not taught across the board.
Mr Gamble: It is not sufficiently well indoctrinated into the National Curriculum and it needs to be part of the personal, social and health education programme as integrated into everyday lessons about child safety. If it is dealt with as an isolated specialism, it will be delivered or not delivered and listened to or not listened to. We are working at the minute on a secondary programme which targets children between the ages of 11 and 12 and 15 and 16. Those are the ones that Ofcom say to us are most likely to have on-line access in their bedrooms or in private. That is this year, a school-year programme. The next one we are looking at, and we are working with all of the partners you would imagine here, is looking at how we engage primary education. Beverley Hughes visited the centre and we met with her officials and, as I said earlier, they are now actively seeking to employ a full-time member of the DfES to work within our education team so that we can further indoctrinate this in a sensible way.

Q235 ***Lord O'Neill of Clackmannan:*** You have the target of reaching a million schoolchildren. It has been suggested to us by the children's charities that this is rather ambitious, hugely ambitious in fact. Given the resources at your disposal, are you confident that you will be able to achieve this figure?
Mr Gamble: It is an ambitious target and we could never deliver it by and of ourselves. We are delivering it by cascading. We have trained 1,355 different teachers, school liaison officers, some librarians and some student teachers in other places and, just as an aside, I think student teachers are the people we need to be targeting most effectively in this area because they are tomorrow's generation of schoolteachers. Those 1,355 cascade that information out into

schools, so a member of staff does not stand in every school, but those local police liaison or local safeguarding body personnel or others who have a relationship go out with the content which we have created and deliver it in the way we have trained them to, so do I think we will make it? Yes, I do. The way we are looking at it at the minute is that nearly 400,000 packs have been delivered to particular schools so far and we have until June, the end of the school year, and I believe yes, it is a big target, but our website is getting three million hits a month. We need to engage children in the right way and in fact if you could say it was banned, we would probably increase that to about 20 million hits a month.

Q236 ***Lord O'Neill of Clackmannan:*** The National Education Network have said that they do not really like the idea of devolving broadband funding to schools because they think this would diminish the good work which has been done on security and standards by the regional broadband consortia and local authorities. What is your view on this? Should Whitehall be intervening in setting standards so that this potential gap is bridged?
Mr Gamble: Well, we work with those consortia and I think that I have to give credit where credit is due and say they have done a great job in a number of areas and we have learnt a lot of lessons about that. I am not sure about the way forward in that regard at all. We need to speak to them, we need to engage with schools and it needs to be a collective discussion that makes sure that, by simply moving from one process with the broadband consortia to another, we do not undermine our ability to deliver a safer infrastructure because that is what might happen if it goes down to the individual school.
Mr Wright: I cannot answer that. It is DfES policy.

Q237 ***Chairman:*** We will have to cut it off there. Thank you very much for your answers. I think it is very interesting listening to you; it reinforces the view that, as you have said, technology is neutral and this is largely a social problem. It is almost ironic to me that the three-dimensional nature of a web means that we do not have fingerprints on images which probably made the old world easier, did it not?
Mr Gamble: But we actually do have fingerprints.

Q238 ***Chairman:*** But you really do not because you do not know where these images have come from in general and it is almost impossible to trace them back to the origin.
Mr Gamble: We can. Through the child-based technology we have, we are able to take 750,000 images, run them through our computer and it will tell us if we know these images or if we do not know them. It will also give us the history of the images that we know. What that does is prevent us from having to spend valuable time in looking at old images so that we are not duplicating effort, so we can fingerprint the image insofar as we can identify it and re-identify it and it is that fingerprinting technology in the IWF.

Q239 ***Chairman:*** That is not what I meant by "fingerprinting". What I meant was that each image would not contain a fingerprint from the person who had sent it originally.
Mr Gamble: And where that does happen is in the more modern digital photography where we are able to get that information, but I accept entirely what you say. I wonder if I could just ask you to bear with me and let me make the four recommendations I wanted to make to you very quickly. The first one I would like to see this Committee ask is that child protection be a national policing priority in the National Policing Plan, and the fact that it is not is a significant problem and I do not know why it is not, but I think this Committee could perhaps bring some focus to that. The second one is that Internet safety be a requirement in the National Curriculum. The third one is that we have a requirement on local safeguarding boards to have designated posts with responsibility to co-ordinate Internet safety across children's services. The fourth one is that you encourage the use of various types of blocking technology to meet the requirements of protecting children, whilst recognising the limitations of some of our industry partners.
Chairman: They are useful suggestions and it is valuable evidence you have given to us and thank you very much.

Supplementary memorandum by Mr Jim Gamble

The Committee have offered me the opportunity to provide supplementary evidence in light of a recent communication to the chairman in relation to the case of R v Grout, where you state my evidence has been challenged. In response, the statement I gave to the Select Committee of Science and Technpology on 10 January 2007, is and remains to my knowledge, a true and factual one.

I am not prepared to highlight specific issues that would disclose sensitive and personal information into the public domain, however there is a need to reinforce the point that individuals can and do perpetuate a view, whilst being selective of the facts and without producing significant evidence. I request you forward us any evidence you may have in your possession or the letter you have received to better inform our process.

You have requested information about the use of the charge of Incitement and what I regard as a sufficient factual and evidential basis for such a charge. This matter does relate to the investigation and prosecution of online child abuse cases and as you have stated, this is not the primary focus of the inquiry, all charging decisions and formulation of charges is a matter for the Crown Prosecution Service in accordance with their guidelines and policy.

However, given the sensitivities around this matter, I feel it would be useful to invite the Chairman to a Confidential meeting to provide him with a further briefing.

23 March 2007

Supplementary memorandum by Mr Jim Gamble

I write further to your letter dated 26 April 2007, requesting clarification of points made in your letter dated 1 March 2007 and seeking answers to a number of specific questions.

OPERATION ORE

In September 1999, the US Postal Inspection Service searched the premises of an American based online trading company known as Landslide Inc. this company was providing access for payment to adult pornography and child abuse images. Material was seized which included a database containing the list of subscribers. In September 2001, following the conviction of Thomas and Janice Reedy, owners of the company, Landslide Inc transaction information was received by the National Criminal Intelligence Service.

Prior to any public statement alerting suspects to the investigation, 50 cases across 31 different police force areas were actioned. The overwhelming majority of these cases led to child abuse images being found on computers.

In September 2002, the National Crime Squad took the responsibility for national co-ordination dealing with the dissemination of the subscriber data. This included a co-ordinated approach to the categorisation and prioritisation of individual suspects based on their potential access to children.

This transaction data consisted of information submitted by a customer in purchasing access to the websites, which included their name, address, credit card number, email address and a customer selected password. In April 2004, following the first incitement case, further forensic work revealed the capture of the subscriber IP address and the credit card verification logs.

In the majority of Operation Ore cases, police forces have used the data from Landslide Inc to commence investigations into the suspected possession of indecent images of a child. Once the individual packages were released to the forces, it was the responsibility of individual Chief Constables to decide whether to undertake investigations. Following investigation, forces considered whether offences had been committed and warranted judicial proceedings; each case was independently scrutinised by the local Crown Prosecution Service (CPS).

To the best of my knowledge more than 2,450[1] individuals have been successfully held to account. This figure presently shows a 93 per cent rate of guilty pleas and includes more than 700 admitting their guilt in receiving a formal caution. In almost 2,300 cases, child abuse images were discovered. In 21 per cent of all dissemination cases, following an investigation, the Police Service took no further action.

Following the publicity generated by some high profile cases and greater levels of awareness that an investigation was ongoing, the CPS developed a response for the occasions where no images were found. A CPS prosecution strategy emerged, focusing on the subscriber incitement of the Reedys to distribute child abuse material. The CPS additionally drew up and issued best practice guidelines.

These incitement cases number only 161. This figure represents 1.8 per cent of the total dissemination of transaction data. In the majority of these cases (68 per cent), the individual admitted their guilt and received an adult caution with placement on the sex offenders register. The remaining cases were subject to court proceedings resulting in 24 convictions and two acquittals. The CPS chose not to proceed in 13 cases. Only 10 contested incitement cases presently remain outstanding.

In these incitement cases, the evidential connection between the personal details provided, the identity of the user and a direct link to a site offering child abuse images is clearly key. This is a matter dealt with on a case by case basis, subject to the particular circumstances.

I will now deal with the questions you have posed in your letter dated 26 April 2007.

[1] The statistics include information supplied by forces in the first instance, with some selection and manual inputting by NCS/CEOP officers in the second. The data has then been cleansed and analysed. Statistics reflect activity to 17 May 2007.

Whether CEOP (or the police prior to the establishment of CEOP) have launched investigations into suspected online child abuse on the basis solely of the use of credit cards online

CEOP has not launched investigations into suspected online child abuse cases in the context of Operation Ore. This is the responsibility for local police forces.

In my experience when an Internet user subscribes to a website offering child abuse images, they provide personal data to a registration page. Similarly to the explanation above, this data may include:

— Name.

— Postal address.

— Email address.

— A personal password.

— Their credit card details.

In addition, the IP address of the subscriber may be captured by the system (the IP address can provide information indicating the address or location of the subscriber).

This information is analysed by the local police who then attempt to identify the particular individual who accessed the site by providing that information. Their enquiries may include: postal address; any previous offending history; existing intelligence or other relevant information; and, whether the credit card was reported lost or stolen.

Whether CEOP (or the police) have sought and been granted search warrants to enter premises and seize materials on the basis solely of the use of credit cards online

CEOP have not sought or been granted search warrants on the credit card information. However, CEOP cannot comment on what other police agencies may or may not have done.

Whether any prosecutions, in particular for incitement, have been brought, in particular under Operation Ore, on the basis solely of credit card information

To the best of my knowledge, in all incitement cases, additional evidence beyond simple single credit card details have supported the prosecution. I understand that where there is doubt, suspects have been given the benefit of the doubt.

In my view, where there is an allegation relating to child abuse (directly or indirectly) it is for the police to establish whether and by whom an offence has been committed, plus to ensure no children are at risk. If sufficient evidence exists and it is in the public interest, a file is submitted to the CPS for their consideration as to a prosecution or otherwise. The evidence is considered by the defence teams and their consultants. The veracity of that evidence is then further tested by the Courts to a standard that is beyond reasonable doubt.

The police are under a duty to disclose material to the defence that either undermines the case for the prosecution or assists that of the defence. This obligation requires the police to pursue all reasonable lines of enquiry including those that point away from the suspect. Failure to comply with these obligations may result in the court refusing to allow the prosecution to continue and staying the case as an abuse of process. Whilst I am unable to comment on the disclosure decisions in individual cases I would expect that once a defendant has raised the possibility of his being the victim of credit card fraud, enquiries would be undertaken in order to ascertain if that was correct.

Whether any investigations or prosecutions are pending and if so, how many under Operation Ore in which the only evidence available is credit card evidence

A number of investigations and prosecutions are pending. No prosecutions, to my knowledge, are pending where the only evidence available is a simple single credit card transaction. As already stated individual police forces are responsible for the investigation of individual cases.

What impact the prevalance of online credit fraud and identity theft (most recently the hacking of TK Maxx) has had in your view of the reliability of unsupported credit card evidence as a basis for launching investigations and prosecutions for online child abuse

This question has been previously addressed. However, I want to reiterate the point, that members of the Committee must be clear on the distinction between an investigation and prosecution. In my view, where such an allegation exists that relates to child sexual abuse, the police are duty bound to establish whether and by whom an offence may have been committed. That investigation in my view would never lead to a prosecution solely on the basis of simple credit card evidence.

I note from your letter, that the Committee mentions a case. This inquiry, to my knowledge, was not proceeded with on the basis of unsupported credit card use, and a number of facts were taken into account by the relevant police service and thereafter the CPS before a decision to prosecute occurred. This matter can be further clarified in writing by the police service concerned if the Committee so wishes.

I note you have chosen to accept Mr Campbell's magazine articles as evidence. I therefore think it appropriate that I respond to some specific issues raised.

Fraud

Although I do not ignore the possibility of fraud, reading the *PC Pro* article, from the information available to me, I can not recognise the article's analysis or outcomes.

Inevitably there will be some element of fraudulent activity on the Landslide Inc. system. I am, and remain, unaware of the "endemic" or "widespread" nature of fraud as suggested in Mr Campbell's article. I believe the proper place to debate the issue whilst cases are outstanding is in a court of law.

Fraud tested in the Courts

In the incitement case of R v O'Shea, O'Shea took Coventry Magistrates Court to judicial review, challenging the sufficiency of evidence to justify his committal to to Crown Court. The High Court sitting in the Royal Courts of Justice dismissed the application, stating that details of email, postal address and credit card were sufficient for a jury to draw the conclusion, if so minded, that the person with that identity was the person who had keyed the information into the computer.

In "C" v Chief Constable of "A" Police and "A" magistrates court, "C" sought that the police should formally acknowledge that there was no case against him and stop their Operation Ore instigated investigation. Albeit the local police did receive some criticism, rather than an apology, the High Court determined it had been reasonable for the police on the basis of the information disseminated and developed by them, to commence and continue an investigation. More specifically, the High Court found that the claimant's case fell far short of establishing that the police were bound to conclude that the claimant was a victim of identity theft. The lead Judge emphasised that what is perhaps a possibility should not be presented as a probability.

Kean Songy's post mortem report

In relation to Mr Campbell's account of a post mortem study of Landslide, CEOP have obtained a statement from Mr Kean Songy. Songy states he had a limited conversation with Mr Campbell. He denies the assertions attributed to him, stating a review of credit card activity prior to the police search of Landslide Inc. does not translate into a post mortem study. Mr Songy cannot understand how Campbell has reached his conclusions. We note that Kean Songy suggests one of the possible options is that there was no fraud.

Defence access to the hard drives

Following the copying of the Landslide Inc hard drives in October 2002, responding to CPS advice in meeting disclosure guidelines, arrangements were made for their examination by defence representatives. In providing the appropriate environment and facilities, two independent defence examiners were consulted. For the purpose of contested cases, defence representatives, including Duncan Campbell, have visited the examination facilities on numerous occasions.

As the original material includes the abusive images of children, evidence of linked prosecutions, details of persons suspected of offences not yet dealt with and potentially information identifying innocent people, defence representatives were asked to sign a confidentiality agreement. Again, Duncan Campbell has signed such a document.

In the case of R v Bird, the defence counsel using Mr Bates' services requested a copy of the entire database. Judge Baker agreed the defence team were permitted to inspect the Landslide Inc. system. However he was not persuaded that Mr Bates' lack of familiarity with Linux justified a full copy of the system nor that he was unable to conduct the work required save only at his own home.

Belfast Crown Court

The defence produced a hand written note, requesting that parties exchange details of approximately 250,000 files on Landslide Inc. computers. This exchange was to include hash values of the hard drives, but not the content. This indicated to the prosecution team that the author of this document has access to the hard drives from Landslide Inc., potentially including indecent images of children.

This note therefore may be evidence of an offence. As such, the PSNI on behalf of the prosecution declined to return it to the defence team. As soon as the Judge offered to retain the note, the PSNI officer co-operated with the court, exhibiting it as evidence of an offence and leaving it in possession of the court.

Consideration was given as to whether Mr Campbell should be cautioned. A caution is not a threat. A caution is designed to protect an individual of whom there are grounds to suspect an offence may have been committed.

If an individual claims to have copies of the Landslide Inc. hard drives, clarification is required to determine what they have and whether it has been obtained in accordance with the law. If their material includes abusive images such individuals may well be committing a criminal offence.

CEOP are aware that Landslide Inc. transaction data has been released and distributed. This distribution is unauthorised. This information includes details of persons eliminated from enquiries and suspects who have yet to be dealt with. In my opinion, any unauthorised public release of this data is irresponsible, risking public identification of such individuals and potentially obstructing policing activity.

Co-operation

I am aware the CPS in relation to Operation Ore disclosure obligations has written to both Mr Campbell and Mr Bates seeking information that would undermine the Ore generic evidence. I am advised to date Mr Campbell has provided no credible information. Mr Bates has not replied to their requests.

In Conclusion

In preparing this letter, I have tried to balance the public nature of the Committee's work with the sub judice of outstanding prosecutions. It is also difficult challenging points made without abusing the parliamentary privilege.

I hope this letter whilst answering your questions, provides further clarity on Operation Ore. Should you wish further evidence, I am willing to attend your convenience in person.

1 June 2007

Memorandum by the Children's Charities' Coalition on Internet Safety

1. The Children's Charities Coalition on Internet Safety (CHIS) brings together the UK's leading independent child welfare and child protection organisations to focus on making the Internet a safer place for children and young people.

2. Below is our response to the questions on Internet security which the Select Committee has posed in its Call for Evidence.

Defining the Problem

3. The Internet has brought immense benefits to society in general and to children and young people in particular. That said, there are clearly also serious downsides to the Internet as far as children and young people are concerned.

4. The Internet is increasingly recognised as being a public space but, at present, there is a widespread feeling that there are still too few protections for children and young people within it. Indeed for some children the Internet has become an additional medium through which they can be bullied, harassed, threatened and made to feel unsafe.

5. Wonderful though its many other attributes are, a major unintended and unforeseen consequence of the growth of the Internet as a mass consumer product has been the emergence of categories of risk which hitherto were either completely unknown or were much more limited in their scope. In relation to children and young people, many of these risks are poorly understood by parents, teachers and others with a responsibility for supporting children through the different stages of their development into adulthood. Even when the risks are understood at a general level, there is often a very limited appreciation of what practical steps could be taken to reduce or minimise them.

6. In a survey conducted for NCH earlier this year, ICM interviewed a thousand children aged 11–16 and roughly the same number of their parents.[2] One third of children surveyed said they regularly used blogs, yet only 1 per cent of their parents knew that they did. In fact two-thirds of parents did not know what a blog was. Similarly 79 per cent of children said they used Instant Messaging regularly, yet only one third of parents understood what Instant Messaging was.

7. Without doubt this lack of awareness of some fairly basic aspects of children's and young people's use of the technology on the part of parents is rooted in the fact that many of them left school before the Internet became what it is today. Parents have not had the same opportunity to gain a similar level of familiarity with the technology as their children. This more limited knowledge means parents may struggle to help their children understand or deal with the risks that the new technologies present.

8. There are two principal security threats to children and young people posed by the Internet. Firstly it can facilitate their exposure either to egregiously age inappropriate content which they may find disturbing or distressing. Secondly it can also expose them to predatory individuals who mean to harm or exploit them.

9. The Select Committee might also want to note that some banks issue, for example, Solo card, to children as young as 11. These can be used to make online payments. As the Trading Standards Institute has noted, since a reliable visual check of a person's age is, for practical purposes, impossible on the Internet, this has meant that children and young people have been able to obtain access to age restricted goods or services in circumstances which would not have obtained in the real world eg they have been able to gamble, buy knives, alcohol or tobacco, or adult videos. In addition, children and young people have also been the victims of frauds which would not so easily have succeeded had the targets been worldly wise adults.

10. Addressing the security threats to children and young people outlined above is not only vital in its own right, from a child protection standpoint, but it is also important because of the impact any well-publicised failures have on the general level of public trust and confidence in the Internet. A medium that is so frequently associated with stories about child pornography, paedophiles and scams of various kinds is one that many will choose to avoid.

11. A startling illustration of this enduring lack of public confidence in the Internet was supplied in a MORI poll carried out for *The Sun* in January 2006.[3] Entitled "Britain Today" it showed that, given a very wide range of choices, two out of the top five worries of adult Britons concerned children and the Internet. Whatever view one might take about the empirical basis for such a level of concern[4] there is no denying, firstly, that it is grounded in real events that have happened to real children and, secondly, that it persists.

Tackling the Problem

12. In the UK we are fortunate to have the recently established (April 2006) Child Exploitation and Online Protection centre (CEOP). CEOP has recently launched a hugely ambitious programme to reach, through the schools system, one million children to present them with safety messages about online risks. In this endeavour, CEOP is working very closely with and in many ways is building on the excellent work being done by the British Educational Communications and Technology Agency (Becta), a standalone organisation which is a major source of advice and guidance both to the DfES and individual schools.

13. Running alongside CEOP's and Becta's work are the activities of the great majority of consumer-facing Internet Service Providers, mobile phone companies and portals which similarly put a great deal of effort into publicising key safety messages aimed at children and young people. Through their web sites and other outreach efforts, many of the children's charities themselves also make their own modest contribution to this larger effort. In our view all of the players in this space have been greatly encouraged by the strong leadership shown by and through the Home Secretary's Internet Task Force on Child Protection, first established in 2001.

[2] See http://www.nch.org.uk/information/index.php?i=77&r=469

[3] See http://www.mori.com/polls/2006/s060117.shtml

[4] Official figures are not always very helpful in allowing anyone to make judgements about the scale of the problem, much less to make comparisons with pre-Internet days, but two reports which, *inter alia,* present some of the data to do with child sex abuse on the Internet and child pornography have been submitted separately to the Select Committee. These are "Child Abuse, child pornography and the Internet" (2004), and "Out of Sight, Out of Mind" (2006), both published by NCH.

14. So far much of the effort referred to above is directed at increasing children's and young people's awareness of the risks and how to deal with them. There has also been work directed at building awareness and capacity among parents, teachers and others with responsibilities for children and young people, but we need to do a great deal more to reach out to these latter groups. As explained above, parents in particular need to be much better equipped if they are to be able to provide appropriate and timely support to their children.

15. While all members of CHIS are committed to the idea and importance of awareness raising and education initiatives, we also believe there will inevitably be limits to what they can achieve. We know there are some hard to reach children and families for whom, whether temporarily or for the longer term, education and awareness initiatives will either be entirely irrelevant, entirely inadequate, or of very limited value. Children with certain kinds of learning difficulties or behavioural problems, or children and young people who are unusually needy for any number of possible reasons, might derive little benefit from a web page full of good advice. Constant supervision is one possible answer, but that is not always going to be available or practicable.

16. This leads us neatly to a second qualification: while education and awareness are key tools, in the quintessentially technical environment which is the Internet we are very clear that improved technical solutions can also play an enormous part in helping to keep children and young people safe.

17. The high tech industries are deploying ever more sophisticated solutions to combat spam, hacking, phishing, identity theft and all the other familiar problems which bedevil the Internet. We can see no reason why child protection should be exempt, and indeed some companies have been devoting a great deal of time, energy and research resources to this issue, particularly in the field of filtering technologies. We welcome these moves and look forward to their deployment on a much larger scale than we have witnessed up until now. For example, we believe that a filtering product should be preinstalled on every computer sold into the domestic market, and it should be set by default to a high level of security. This is something we have campaigned for in the past, and we continue to do so. Such a product could be turned off altogether or the settings could be modified if the user so wishes. However, it seems to us entirely wrong that computers are sold into the domestic market with, essentially, haphazard arrangements being made in terms of ensuring that parents understand the risks and what to do about them. So far only one UK manufacturer of PCs has followed the view expressed here and that was Comet, the electrical retailers. This shows that it can be done, if there is a will.

Governance and Regulation

18. When one looks across the globe there is little doubt that within the cohort of liberal democracies the UK stands out for both the scale of activity in this area, and its apparent effectiveness. For example, witness the reduction in the volume of child sex abuse images being published out of the UK, from 18 per cent of all illegal images in 1997 to less than 0.4 per cent today. Similarly, pioneering initiatives such as BT's Cleanfeed are now being taken up in several other countries.

19. It is hard to prove this beyond all reasonable doubt but it is widely accepted, and justifiably so in our view, that the UK's self-regulatory regime has played a major part in allowing the child safety agenda to move as far and as fast as it has. Again, we believe the Home Office Task Force has been absolutely pivotal in this respect.

20. At present CHIS is broadly happy with the current self-regulatory regime, although it is an area of policy which we keep under constant review. We think there are many important things that still need to be done, urgently, many of which will increasingly depend for their success on improved international co-operation.

21. We would like more thinking to be done about how to develop the international political will and leadership to tackle the kinds of challenges that can no longer be addressed domestically eg around the continued growth of child sex abuse images on the Internet. We doubt that shifting domestically, for example towards a more dirigiste regime, would materially aid the situation. Indeed it is likely to make it worse. One volunteer is worth 10 pressed men.

Crime Prevention

22. In the field of child protection we have several on-going concerns in terms of law reform and these are being pursued within the framework of the Home Office Task Force.

23. Although it is too early to judge what difference CEOP will make to the overall situation within the UK, we all have high hopes and expectations, and are fully supportive. We believe the early signs are very promising. We will be monitoring CEOP's activities closely and look forward to engaging with and supporting their future activities.

24. We are not sure if CEOP has the right level of resources to allow it to deliver its very ambitious programme of work. There is little doubt, for example, that there has been insufficient investment generally in the police's forensic capabilities. The delay in analysing suspects' computers after seizure is still far too long in far too many forces and in far too many cases.

25. More generally we are aware that the rate at which police officers are being trained to work in these high tech areas is still painfully slow and more resources would probably help speed this up.

26. The leading role the British police have played on the global stage in this field ought to be recognised and applauded. However, there are still too many countries which lag a long way behind and this is bound to remain a major obstacle to progress. Interpol, Europol, G8 and the Virtual Global Taskforce need to give more attention to this problem. Ways should also be found to allow civil society to be drawn into and support the work of law enforcement internationally.

Examination of Witness

Witness: Mr John Carr, Executive Secretary, Children's Charities' Coalition on Internet Safety (CHIS), examined.

Q240 ***Chairman:*** Mr Carr, thank you very much for coming to talk to us. You have been sitting there, so you have seen how we proceed. Would you like to introduce yourself, first of all.
Mr Carr: I represent the Children's Charities' Coalition on Internet Safety. That comprises all of the UK's largest child welfare charities and child welfare organisations, the NSPCC, Barnados, NCH, the Children's Society and so on. I am technically an employee or a consultant, I should say, to NCH and their contribution to maintaining the coalition is, as it were, to lend me as a resource to it, so I am an independent consultant, I work for the children's organisations, but also for other people as well, and I have been working particularly in this area of child protection on-line for just over 10 years now.

Q241 ***Chairman:*** Is there anything you would like to say as an opening statement?
Mr Carr: Beyond that, no. I endorse certainly the recommendations that I just heard the police make; I think they are sound and would be very useful, particularly the first one about getting child protection made a national policing priority and it is a mystery why it is not.

Q242 ***Chairman:*** Let me start by opening up questions for you and the first one is: who do you think is responsible for protecting children on-line?
Mr Carr: There is no silver bullet, there is no one agency or group which has this responsibility exclusively. I think the industry certainly has a key responsibility, and that covers a range of different players. The education system absolutely has a responsibility, as it does to educate children about a whole range of civic and personal things within the context of education. Of course the Government and the public services have a responsibility in terms of promoting a healthy society to make their part, make their contribution to that process. Again, just to underline the point that was made before, parents, above all, have a responsibility and children themselves do as well.

Q243 ***Chairman:*** Do you have any thoughts about what we should do about this? You have identified a significant gap between what children are doing on the Internet, blogs and instant messaging, et cetera, and the level of knowledge of parents, who in most cases have never even heard of these technologies.
Mr Carr: Yes, without a doubt, I regard one of the most important things that public policy needs to address is how we close that gap because parents are always going to be the first, and best, line of defence and support for their children. No-one knows or no-one ought to know a child better than their parents do and no-one is going to be in a better position to help a child deal with a whole range of things, but if the parent lacks the knowledge of certain fundamental things or things that their children are doing, it is very hard to see how they are going to be able to help their child to the best effect, so bridging that gap is a huge challenge for public policy. We, as NCH, were commissioned by the DfES two years ago now to run, and this addresses a question I heard you ask earlier, Internet safety classes for parents working through individual schools and we in fact set these things up in 200 schools in different parts of England, in middle-class, rural areas, in inner-city areas and so on, and the response was very, very diverse. At some of the events we turned up to, one parent came along. At other schools, 250 parents came along. Schools are the logical or obvious way to try and reach out to parents, but the attendance of parents at these sorts of events seemed to depend largely upon how successful the PTA in that school was in attracting parents to a whole range of other things as well. It seemed to me that relying only or even principally on schools as a means of reaching parents to help them bridge that gap was not going to work because you would be in effect devolving the responsibility to agencies that we already know are very patchy in terms of their effectiveness, so

obviously it would be worthwhile continuing to try and make that work better, but we also need to find other ways of reaching parents as well.

Q244 ***Lord Harris of Haringey:*** In your evidence, you refer to two principal security threats, exposure to what you describe as "egregiously age-inappropriate content" and then the exposure to predatory individuals. Can you give us some sort of indication of the risks, the relative frequency and the gravity of it?
Mr Carr: This may shock some of you, but I am in my 50s now, I know I do not look it, but I can remember with crystal clarity the first time I saw what you might generally call a "hard-core" pornographic image. I was 19 years old and I was on holiday in Denmark. Now, that type of image, and I still have a vivid recollection of that particular image because I had never seen anything like it before in my life, that type of image is now kind of commonplace on the Internet. I will give you numbers in a second, but it is seen not infrequently by children as young as six, seven, eight, nine and so on. There are a whole range of possible views that one might take about how bad the impact of those types of images might be on children. Some people think they are absolutely inconsequential and that they do not do any real damage at all. Others, and I would associate myself with this second category, think that this can be very scarring and very damaging and very shocking particularly for younger children to be exposed to. Just to turn to the numbers, the most authoritative source of data, by the way, in this field is, without doubt, the survey done by Professor Sonia Livingstone of the London School of Economics and I ought to make clear that I was a member of the advisory group that helped devise this survey and helped as an adviser generally with that project. What they found in the LSE survey, and this is all available on-line in a publication called "UK Children Go On-Line", was that 57 per cent of youngsters between the ages of nine and 19 who were regular users of the Internet had come into contact with on-line pornography and 38 per cent of those had seen it as a result of pop-ups that had appeared on their screens, so again unsolicited, unsought, unlooked for, 36 per cent had found it accidentally and 25 per cent had seen these types of images as a result of opening up spam which they had received, unsolicited email. The scale and frequency is not, I think, really in dispute any more. One would hope that, as anti-spam technology improves, as the messages get through about the importance of not opening spam if you do not know the source and so on, these will reduce, but I still think that, however successful those sorts of initiatives are likely to be, the residual component of that type of activity is still going to be substantial. How scarring and how bad could the exposure to this type of material be for an individual child? It is very hard to say because these are subjective things and there are no objective criteria that you can refer to that are of any great assistance. For a particular child seeing a particular image in a given context, it may have very little effect, but at another time being exposed to those sorts of images, for a different child, a more sensitive child, a more sheltered child, it could be very, very damaging indeed, very scarring indeed. I am happy to develop on that if you want me to, but I will move on now to the question of contact and communications. Again if I refer to the LSE study, one third of regular users of the Internet between the ages of nine and 19 said that they had received unwanted sexual messages and 31 per cent said that they had received "nasty comments" on-line or through their mobile phones. In this study, by the way, which was done face to face where they interviewed the parents of the children afterwards and separately, only 7 per cent of the parents were aware that these types of things were happening to their children. A significant proportion, in the LSE study again, around about 8 per cent of children who had met people for the first time on-line went off to meet them in real life. Now, that is obviously potentially the most risky thing that can happen, a child meeting somebody in a chatroom or in a virtual environment and being invited to go and meet them in real life and then actually going off to do that. There was one case which was documented by the University of Central Lancashire where I think a nine-year-old boy, who lived in Preston, went off to meet somebody whom he had met on-line and got on the bus and went to Blackburn to meet the person. As it happens, it turned out they were both great football fans of Manchester United, so nothing bad came of it, but it does illustrate the possibilities that can arise from this.

Q245 ***Lord Mitchell:*** You have advocated the compulsory reinstallation of filtering systems on computers, and the police have called them "nanny programs", to be set at a high level of security. Do you have any measure of the effectiveness of such filtering systems?
Mr Carr: The short answer is no, but we will do soon. The Home Office speaker previously referred to the fact that there is a government working party, of which I am actually the Chairman, by the way, which is looking into developing a kite-mark, working with the British Standards Institute to give a quality assurance mark for filtering products.

Q246 ***Lord Mitchell:*** Do they work?
Mr Carr: Yes, they work. The question which we have not yet finally resolved is what numerically will be an acceptable level of false positives essentially, which is what it will come down to. We would hope

that the filtering software will work at the same type of level of efficiency as anti-spam and anti-phishing programs already do. Whatever filtering program that you might imagine will be used in this environment is never going to be 100 per cent perfect; it will over-block or it will under-block. The question is: what is an acceptable level?

Q247 ***Lord Mitchell:*** If I wanted to turn on anti-spam on my computer, I would be doing it because I wanted to do it. If a parent turns it on, the parent knowing probably a lot less than the child as to how the computer works, the child can then turn that off quite easily presumably.
Mr Carr: Only if the parent has done it badly. Sadly, it is worse than that because typically what will happen is that the parent will say to the child, "Here's the blocking software. Would you mind installing it, please", so the child will invent the password or, alternatively, the parent will tell the child the password. This gets to one of the issues and one of the problems with the blocking software, that the software has to be very good, otherwise parents will simply turn it off. If a parent is being called up to the child's bedroom or study every five minutes because a site is being blocked and the child cannot read it and the parent needs to make a decision about whether to override it or not, they are going to get fed up of that pretty quickly and they are going to stop using it, so the software has to work at a very high level of efficiency and be very smart. Some of the software products which came out in the early days were very poor and that is why the take-up of them, in part at any rate, has not been as good as it might be. What we hope is that, if we develop a BSI standard which will be on the boxes in the shops or on the websites when parents go to it, when parents see that BSI kite-mark on the products, this will give them some level of confidence in the quality of the software and it will encourage them to download and use it. I might just say, you asked a question earlier about what the response from the industry has been, and obviously the manufacturers of this software are very keen on this initiative because they imagine it will mean that their products will sell more, but the really difficult bit of the equation is getting the computer manufacturers to agree to the pre-installation because it is at the factory where these settings are first put on the machine. One manufacturer has already done it and that was Comet. Now, Comet are a major electrical retailer, they are not major computer manufacturers, but they do have their own brand, they are a manufacturer of computers and they did do it on their own-brand machines. That demonstrates that it is possible, but only if you want to do it. The cost of doing it is negligible. I went to the factory to see the whole process being done and the manager of the factory that I visited said quite frankly that it is impossible to compute the cost of that extra step in the manufacturing process because, in essence, all they do is make the settings once, they put them on the goldmaster disk and that goldmaster disk is then copied along with everything else, the operating system, the office software and what-have-you, on to the hard drive, so in terms of additional cost in the manufacturing process, it is nearly nil.

Q248 ***Baroness Sharp of Guildford:*** In your evidence, you express support for the UK's self-regulatory approach, but are there areas where you think regulation might be more appropriate?
Mr Carr: No, but a qualified no. Self-regulation is always going to be a better approach because it is more flexible and quicker. Leaving aside acknowledged national emergencies and so on, if you look at the typical gestation period for an idea coming into the public policy arena and ending up as a law, it will typically be four or five years or something like that. If you have a self-regulatory environment, it is possible to move a lot more quickly and of course self-regulation, by definition, means that you have got the co-operation of industry and, if you have got the co-operation of industry, then you have got access to their expertise and they are going to be much more enthusiastic about getting on and doing it. Self-regulation has worked very well in the UK up to now, but I have to say, and I do not want to be disingenuous about this, I think one of the reasons it works so well is because the industry believe that, if self-regulation is not seen to work, the Government will step in and legislate, and that is what they want to avoid and for very well-known reasons that we need not rehearse. It is very much in the industry's interest, I believe, to continue to make the self-regulatory environment work.

Q249 ***Earl of Erroll:*** How does the risk of going on-line actually compare to the general risk in society?
Mr Carr: Of living, you mean?

Q250 ***Earl of Erroll:*** Yes. There is a risk out there anyway of children being kidnapped and abused, et cetera, but is that risk greater on-line?
Mr Carr: Well, I do not mean to be facetious, but more people get killed falling down stairs every year than do, I think, crossing the road or something of that kind, but do we all live in bungalows? No, we do not. If you are a parent and you are aware of an avoidable risk to your child, you will want to avoid that risk if you reasonably can, so in that sense, whether the risk is one in 10 billion or one in 10,000 or one in 100, it is irrelevant from your point of view as a parent. What you want to know is: is my child at risk, what is the risk and how do I avoid it? With the Internet, what we are talking about are a number of risks which are, to a greater or lesser degree,

avoidable and that is why the search is for solutions which help minimise, or eliminate, these risks.

Q251 ***Earl of Erroll:*** I suppose I was thinking of how does the frequency of abuse as a result of someone they have met on-line compare to the abuse which comes from friends, family and neighbours, which we actually know is significant as well? Do we have any figures on this?
Mr Carr: There is no comparison between the two. The level of abuse in real life far, far outweighs and outnumbers the number of cases of on-line abuse of children, as far as we are aware, if I can put it that way. Let me, however, issue one caveat. First of all, the way the crime figures are collected does not help us with an objective determination or in providing an objective answer to your question. I think I am right in saying that even today in the crime statistics it is not recorded whether or not a computer was a key part of the way in which the crime was committed. For example, if a child is sexually abused as a result of an on-line contact, it will not show up as an on-line offence, it will simply show up as a contact offence. We do have some numbers which we can point to relating to child pornography offences and I have published them in a document which came out two years ago. If you look at the incidence of child pornography offences, the line is absolutely straight up and correlates almost entirely with the growth of the Internet. That is not to say that the Internet is the cause of child pornography, it has been around for centuries, but what is undoubtedly true is that the Internet has provided a readier means of people with a latent, or already acknowledged, interest in child pornography to act upon it and gain access to it, and the numbers are very striking and there is no doubt that the Internet has played a part in facilitating that growth.

Q252 ***Baroness Hilton of Eggardon:*** Several responses have mentioned bullying as an on-line issue. Have you any idea about what the incidence is?
Mr Carr: We do. At NCH, we carried out a survey which was in 2005 and those are the figures I have here, but we did a kind of check last year as well and they were broadly the same. Bearing in mind that the ownership of mobile phones is almost universal amongst the teenage group from about 11 or 12 upwards, what we found was that 20 per cent of all children have experienced some sort of digital bullying, 14 per cent by mobile phone text messaging, 5 per cent in Internet chatrooms and 4 per cent by email, so one in five basically of all children, because they are all on-line and they have all got mobile phones, is being bullied in one way or another through the on-line environment.

Q253 ***Baroness Hilton of Eggardon:*** Bullying is normally by someone that you know or by a group of people that you know, so it is probably more likely to be on mobile phones perhaps where you know who the perpetrators are.
Mr Carr: And the numbers do suggest that.

Q254 ***Baroness Hilton of Eggardon:*** It is not normally a matter that the police can deal with.
Mr Carr: There are potentially three different crimes involved in bullying. One is an offence under the Malicious Communications Act, one is an offence under the anti-stalking laws and one is an offence under the Telecommunications Act, but you are right, that these matters are not traditionally police matters. Perhaps I could just say a word about on-line bullying. When I was a lad in Leeds, there was bullying going on in our school and I can remember being the victim of it myself on one occasion, but pre-Internet, pre-mobile phones a kid knew that, when they got home and they closed the street door behind them or they went up to their room and closed their bedroom door, the bullying stopped and they had found a sanctuary. That is no longer true. The whole point of having a mobile phone is that it is on so that your parents or your mates, whatever, can get you as and when they need to. The whole point of having a computer and the Internet is so that you can use it to do your homework or whatever, but it also means of course that the bullies can get at you 24/7 too, so in some ways it is a very insidious, intrusive development in the way bullying works.

Q255 ***Lord Howie of Troon:*** I am told that there are a number of social networking sites and two names have been suggested to me, with which I am unfamiliar, I have to say, Bebo and MySpace. First of all, what is your general view of these sites and, secondly, do the sites do enough themselves to protect children?
Mr Carr: I should declare an interest here. I made it clear at the beginning that I work not just for children's organisations, but for companies as well and I am an adviser to MySpace, so I have some inside knowledge, as it were, of that particular company.

Q256 ***Lord Howie of Troon:*** Open up then.
Mr Carr: The phenomenon of social networking sites is huge. In the on-line stats which were published last month, I think, MySpace finally overtook Yahoo as the most visited in the United States. MySpace has six million subscribers here in the UK and Bebo has also a very substantial number of members too. The social networking sites in general are not an entirely new phenomenon. What they have done in a very clever way, which is why they have become so popular so quickly, is brought together a number of different

technologies that previously people used discreetly or individually, so you have now got in one place, in a very convenient way, access to video, access to messaging-type services, access to pictures and photographs and they have all been brought together into this single place, so they are very, very attractive and that is why they have been hugely popular with youngsters. All of the social networking sites are very keen to ensure that their users are aware of some of the risks. We heard Jim Gamble earlier speaking about the image of a child walking between Oxford Circus and Tottenham Court Road with a billboard giving all of their personal information to any potential passer-by. That is the kind of thing that could happen on a social networking site and it is why each of the companies that I am aware of anyway is putting a great deal of energy, effort and resources into getting the messages across.

Q257 ***Lord O'Neill of Clackmannan:*** You have raised the question of Solo cards being issued to very young children in the absence of visual checks, which means that they can enter into transactions and the like. What do you think needs to be done? Do you think the banks need to stop issuing them? What would be your answer to this problem?

Mr Carr: I certainly do not think the banks will stop issuing them, and I am an agnostic as to whether they should or not. My own children both got them when they were 11 because we opened up bank accounts for them with NatWest and they were part of the package that they got. What we need is a reliable means of age verification. Children tell lies about their age and they have done since time immemorial. Traders should not take it for granted that people make truthful statements where the product that they are selling is an age-sensitive or an age-restricted one.

Q258 ***Lord O'Neill of Clackmannan:*** So how can service providers do this?
Mr Carr: Well, as you know, the Gambling Bill, which went through last year, has increased the penalties on gambling companies and I think we are going to see similar things happening in other areas of policy as well. It is technically possible to do it, but they need to be made to do it.

Q259 ***Lord O'Neill of Clackmannan:*** I had a son who was once two years older than his older brother!
Mr Carr: There you go!

Q260 ***Chairman:*** Mr Carr, thank you very much indeed. If there are any other thoughts you might have for us, please submit them in writing for us.
Mr Carr: Will do. Thank you.

WEDNESDAY 17 JANUARY 2007

Present	Broers, L (Chairman)	Mitchell, L
	Erroll, E	O'Neill of Clackmannan, L
	Harris of Haringey, L	Sharp of Guildford, B
	Hilton of Eggardon, B	Sutherland of Houndwood, L
	Howie of Troon, L	

Memorandum by Microsoft

EXECUTIVE SUMMARY

1. Our submission sets out our experiences with the risks and mitigations associated with personal use of the Internet. We have considerable experience in this area: Microsoft is one of the most attacked platforms on the planet and we have learned a great deal about the risks and threats for both us and our users on the Internet.

2. We have worked globally to establish a three-part model to tackling many of the issues faced around online safety:

- consumer education—addressed through initiatives such as Get Safe Online;
- technological practices and improvements—such as anti-malware tools, anti-spyware, anti-phishing filter technology in Web browsers, parental controls (to limit the risks of exposure to minors of unsuitable content and/or contact with parties unknown) and the "identity metasystem" (which aims to improve the quality and consistency of identity on the Internet); and
- legal enforcement—including for example the Global Phishing Enforcement Initiative.

3. All three of these areas need to be developed in partnership to impact the problem of ensuring personal security online. Internet security and online safety require an end-to-end approach.

4. Against a constantly challenging and evolving threat landscape, the industry has continued to make good progress, partly as a result of placing trusted computing at the centre of software design. At Microsoft for example our Trustworthy Computing initiative has had a major impact on reducing software vulnerabilities, as evidenced in independent assessments such as UNIRAS/UNICERT. This has been particularly true since the launch of Windows XP SP2 and will be taken significantly further when Windows Vista—the next release of our operating system—is made available in the next few months.

5. Whilst much of the evidence from ourselves and other contributors may well be a disheartening read, we do have a passionate belief in the truly transformational and positive impacts of the Internet. From the obvious—such as e-commerce and e-government—all the way through to the pervasive computing age, which will enable us to live longer, more fulfilled lives in our own homes and communities.

6. This is why we believe it is important for us to work collectively on addressing the issues that threaten the Internet and its positive potential. The Internet is far more than just Web browsers and email: we need to understand, monitor and manage the risks as the Internet increasingly enables new areas, such as TV on demand and home healthcare monitoring devices.

RESPONSE TO THE INQUIRY

7. The Committee has highlighted several areas that it aims to consider in its current inquiry, namely:

- What is the nature of the security threat to private individuals and what is the scale of the problem?
- How well do the public understand the nature of the threat they face?
- What can be done to provide greater personal Internet security? How much does this depend on software and hardware manufacturers?
- Is the regulatory framework for Internet services adequate?
- How well equipped is Government to combat cyber crime? Is the legislative framework in UK criminal law adequate to meet this growing challenge?

We will address each of these areas in turn.

What is the nature of the security threat to private individuals and what is the scale of the problem?

8. Threats to online safety and security continue to escalate. This can range from the innocuous but irritating. It includes the likes of spam messages (of which we block over 3 billion a day in Hotmail/Windows Live Mail), through phishing attacks (aiming to fool users into handing over important personal information, such as online banking details, that will ultimately lead to a financial fraud) to malware, spyware, trojans, viruses and bots.

9. Such attacks can lead to anything from release of personal information from a user's computer or online services, to destruction of all data on a computer, to the launch of denial of service (DoS) and other malevolent attacks on third parties. Building in software-based counter measures to these threats through tools such as anti-phishing filters and anti-malware protection has been a high priority. The recent release of Internet Explorer 7—which includes such features—is a step forwards in tackling these issues. But we also recognise that there will be a need to continue to innovate as the nature of online threats itself evolves and changes.

10. There are also more fundamental issues to consider. For example, more and more home Internet users are utilising broadband (always on) connectivity and wireless networks within the home. Configuring both the broadband and wireless links to ensure adequate security can be a demanding task for users, and presents a challenge in terms of ensuring that no third parties can access their systems. We have ensured that the firewall provided in Windows XP SP2 and in Windows Vista is on by default to help with protecting consumer's PCs in these increasingly common types of environments.

11. Outside of the physical infrastructure of the typical domestic network, typically protected with firewalls and encryption for wireless networks, phishing provides one of the main attack methods to fool people into handing over personal information that can then lead to an identity fraud related crime and other crimes, such as financial fraud. Some estimates concerning phishing indicate a compound annual growth rate of 1,000 per cent. This is why the latest release of Internet Explorer has built-in anti-phishing facilities and why Windows Defender (which helps protect against malware) is included in the Security Center in Windows Vista.

12. The scale of the problem can be seen in figures from the Association for Payment Clearing Services (APACS), which estimates direct fraud losses from online phishing scams in the UK almost doubled in 2005 alone to £23.2 million.

13. Gartner reported that in 2005 four major British banks delayed intra-bank payments between accounts in an attempt to combat phishing attacks. Delays ranged from several hours to one day.

14. One in 20 UK residents has lost money to some sort of online scam such as phishing, according to research commissioned by AOL UK. The survey of 2,000 net users by AOL found that five per cent had fallen victim to scams and had lost out financially.

15. Forrester Research believes security fears have prevented more than 600,000 UK internet users from banking online.

16. As the Internet moves increasingly into powering more and more of the services and technologies around us, we need to continually assess the threat landscape. For example, the BBC reported (2 October 2006) from the "Hack in the Box" hackers conference in Malaysia that hackers know how to subvert Internet-based telephony systems—including for example the predicted ability to intercept call centres (hence obtaining useful personal information that can assist with identity fraud)—and Internet-based television (perhaps leading to the injection of rogue broadcasts, or interference with legitimate broadcasts). With the predicted growth in home-based intelligent devices (such as telemedicine) which will also make use of the Internet, we all need to remain alert to the potential risks and how we mitigate them.

How well do the public understand the nature of the threat they face?

17. Education is a key cornerstone in combating some of these issues. We provide our own guidance to consumers[1] and also are very active supporters in the UK of the "Get Safe Online" campaign[2] which aims to educate consumers on the risks of the Internet and how to mitigate and manage them. According to a Get Safe Online survey:

- Over three quarters of the UK's population (83 per cent) do not know enough about protecting themselves online.
- 22 per cent of people admitted to opening attachments from unknown sources—one of the most common ways of spreading computer viruses.

[1] http://www.microsoft.com/athome/security/default.mspx
[2] http://www.getsafeonline.org/

— Only 15 per cent of people felt they had a personal responsibility to protect themselves from online crime—yet almost one in five British people feel so under threat from Internet criminals they give online crime a higher fear factor than physical crimes like car theft and mugging.

18. To help ensure better public awareness of the risks and their mitigations, we have helped with the sponsorship and development of initiatives such as Get Safe Online and guidance on our own Websites. These resources provide a wealth of consumer education to help online users understand the risks online and better protect their identity information and related personal information. We have also engaged more directly, with our UK staff visiting schools to find ways of better communicating these important messages in ways that really connect and have an impact.

19. One of our most experienced colleagues in online risks, Linda Criddle, has recently published a book "Look Both Ways: help protect your family on the Internet" combined with a Web site[3] that we recommend to the Committee.

What can be done to provide greater personal internet security? How much does this depend on software and hardware manufacturers?

20. Consumers need to be well informed about the reality of the risks presented by the Internet. This needs to be done in practical, pragmatic ways that enable them to manage risk in such a way that they can enjoy the benefits of the Internet, but minimise its negative aspects. This requires continuing education programmes of the kind already in place, perhaps supplemented by good practice guides supplied with new equipment used for Internet access.

21. There is often an inherent tension between making things simple and intuitive for users and ensuring strong security and online safety measures. The industry continues to make good progress in improving the layers of protection available in both hardware and software. But the consumer is an essential part of the solution and needs to understand the options available and how best to deploy them. Neither is the threat landscape static—it constantly evolves, requiring consumer education and awareness to be an ongoing process.

22. Some of the measures we have taken at the technical level include making anti-malware and anti-spyware software available for consumers, adding in a firewall to our products, working with others on tackling the problem of spam and dropping support for online chatrooms. We have also added in additional features to the next release of our operating system, Windows Vista, which include User Account Control (to prevent rogue/stealth software installing) and parental controls. We have applied some of the same models to our other products, including Xbox/Xbox 360 which likewise includes parental controls. We have also focused on making it much easier for non-expert consumers to find and use and manage these functions.

23. Windows Defender for example is a free program that helps protect a computer against pop-ups, slow performance, and security threats caused by spyware and other unwanted software. It features a monitoring system that recommends actions against spyware when it's detected and minimises interruptions. Regular updates are made available automatically to the software enabling it to remain responsive to new threats.

24. The new release of our operating system, Windows Vista, has witnessed a major focus on and investment in additional security. These features to help better protect users include:

— Better protection against spyware—The antispyware software in Windows Vista, Windows Defender, helps prevent computer slow down, privacy loss, and unwanted pop-up advertisements caused by spyware and other potentially unwanted software.

— Safer browsing with Internet Explorer 7 Protected Mode—This Windows Vista-only feature limits Internet Explorer 7 to just enough permissions for a consumer to browse the Web, but not enough to modify their files or settings—which helps keep their computer safe from Web-based attacks.

— More safeguards from Windows Security Center—The Windows Security Center notifies consumers and helps them take action to correct a problem when their security software is not up-to-date or their security settings are potentially unsafe.

— In Windows Vista, the Windows Security Center is improved to include information about their antispyware software, Internet Explorer settings, and User Account Control settings.

— More control over what programs can do—By default, Windows Vista runs programs in a more secure mode. When most applications attempt to perform a potentially dangerous operation that requires administrator privileges, Windows Vista asks the user for their active consent before allowing that program to run. This helps reduce the impact of viruses, spyware, and other threats.

[3] http://look-both-ways.com/default.aspx

— An anti-phishing filter to help protect online identity—Internet Explorer 7 with Windows Vista includes a filter that advises a consumer when Web sites might be phishing in an attempt to steal their confidential information. The filter checks a list of known phishing sites that is updated several times an hour—and can also spot suspicious sites that are not in the database yet.

— Clear Internet history with one click—The sites visited and the information typed when you browse the Web are stored in many different places within a computer. In Internet Explorer 7 with Windows Vista users no longer need to go multiple places to remove their personal information. With the Delete Browsing History feature a user can clear all their browsing information with one click.

— Back up and restore settings, files and applications—Windows Vista provides a more comprehensive and easy backup tool than the basic backup utility included in Windows XP. The new Windows Backup feature gives a consumer more choices for storing their backed-up information and they no longer have to remember to regularly back up their data. Consumers can use a simple wizard to schedule when and where they want everything backed up.

— Parental Controls—Windows Vista introduces a rich and powerful set of parental control features to help parents monitor, manage, and administer their children's computer use—and help keep them safe.

— Review detailed activity reports—Windows Vista can generate a detailed activity report that shows exactly what children have been doing on the computer, including the games they played, the Web sites they visited, and the programs they used.

— Set Web restrictions—Users can use an online service that comes free with Windows Vista to restrict the types of Web sites a child can visit. A parent or carer can restrict Web sites by category, such as blocking all pornographic sites or all gambling sites, or they can block specific Web sites by URL. These restrictions work with most Web browsers.

— Help control the games a child plays—Windows Vista makes it easy for a parent or carer to designate which games their children are allowed to play. They can choose to: Allow or restrict specific games titles, limit children's play to games that are rated at or below a certain age level, block any games with certain types of content they do not want children to see or hear.

— Set computer time limits—With Windows Vista it is possible to set limits to when a child can use the computer and for how long.

25. Many of the problems facing consumers on the Internet have their origins in the fact that the Internet was built without an identity layer. It is difficult for users to establish the authenticity of remote parties that they are communicating with—and difficult to establish their own identity when challenged to do so. Microsoft has been working with a broad industry coalition to distil a proven, empirical set of principles for successful identity based on the lessons the industry has learned over the last 30 or so years. These principles are intended to help bridge the divide between policy aspirations and lower level technical implementation details—and hence provide a critical part of the overall infrastructure required to tackle the problem of the missing identity layer of the Internet. These principles are currently referenced as the 'laws of identity' (laws as in scientific principles). We do not claim perfection or any uniqueness of insight in these 'laws'—but do believe they provide a constructive basis for discussion and debate on ensuring the proper scope of identity systems that will prove sustainable and robust in the long term. And by tackling these issues, we will make attacks such as phishing harder to execute successfully.

26. These "laws" are included for reference at Annex A to this paper. In brief overview, they encapsulate the following elements of good identity system design:

— identity systems must only reveal information identifying a user with the user's consent;

— the solution that discloses the least amount of identifying information and best limits its use is the most stable long-term solution;

— identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship;

— the identity system must support both "omni-directional" identifiers for use by public entities and "unidirectional" identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles;

— the identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers;

— the identity system must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks; and

— the identity system must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.

27. A key part of our work has been ensuring a wider industry consensus in tackling the problem. We have a project known as CardSpace at Microsoft which aims to help provide the missing identity layer of the Internet and which embodies these identity principles in technology. Importantly, a project known as InfoCard is taking place across the industry (including across open source, Java, the Firefox browser and Apple Mac communities). We have been working collaboratively right across the industry to address these identity issues since they need to be solved in partnership if we are to make significant progress on providing the missing identity layer that the Internet so urgently requires. The InfoCard initiative will help remove the over-dependency on user ID and password—one of the most vulnerable problems on the Internet—and move us towards a more secure and more intuitive model.

28. Alongside these industry efforts to improve the online identity layer, we have also been making other technological improvements, such as a new anti-phishing filter in Internet Explorer. This helps users identify suspect Websites, enables easier reporting of suspicious sites—and uses visual cues to warn users when problems have been detected.

Is the regulatory framework for Internet services adequate?

29. Microsoft believes that effective regulation of security in an online world is best achieved by promoting a self-regulatory environment. We feel that consumer demand for security provides enormous market-driven incentives for innovators to work towards new solutions to security threats.

30. Promotion and support of a self-regulatory environment in which innovators have freedom to develop appropriate solutions to address security concerns is vital. Threats to security evolve over time. Only where there is scope for innovation will we see the development of new technological solutions to move towards secure networks. Self-regulation preserves consumer choice and ensures a progressive response to security threats, not limited by rules that may rapidly become outdated.

31. A good example of self-regulation is what has been achieved by Government, NGOs and the industry working together in helping to tackle child safety online. Along with other industry players and NGOs, we sit on the Home Office Child Safety on the Internet taskforce which allows for all participants to openly understand and discuss how we can best ensure child safety online. Microsoft works closely with the Internet Watch Foundation and uses its recommendations to block websites through MSN and Windows Live search.

32. We also joined together with a number of police forces around the world including the UK Child Exploitation and Online Protection Centre (CEOP) to deliver a new technology, the Child Exploitation Tracking Scheme (CETS), which allows police forces to share and analyse information for investigating child sex offences.

33. Our Vice President of Trustworthy Computing, Scott Charney, published a paper entitled "Combating Cybercrime: A Public-Private Strategy in the Digital Environment" as a result of work undertaken with the United Nations. This paper provides an overview of the inherent security and law enforcement challenges of the digital age, and outlines why neither traditional models of government protection nor a purely market-based approach to security is sufficient in the virtual world. It also discusses five elements of a sound public-private sector partnership strategy, using Microsoft's experience to illustrate the roles that industry and government can play in pursuing the strategy. We would be happy to provide copies of this paper to the Committee if it would be useful.

How well equipped is Government to combat cyber crime? Is the legislative framework in UK criminal law adequate to meet this growing challenge?

34. Where we do believe that Government can play a legislative role is in ensuring that they equip law enforcement agencies with a robust legal framework and resources to effectively tackle cybercrime.

35. In this vein, we supported the adoption of the EU Framework Decision on Cybercrime and the update to the Computer Misuse Act which changed UK law in line with this Decision. What we think is extremely important is that the police are given the resources and training to maintain the necessary technical expertise to help them successfully pursue cybercriminals.

36. In the UK, one issue that needs addressing is the problem that cyber crime and related fraud are not presently priority indicators for the police as set by the Home Office. With the changes around SOCA, the proposed re-structuring of police forces and the disappearance of the NHTCU it is unclear how cyber crime and reporting mechanisms are being systematically addressed. There is no single reporting mechanism in the UK (as there is in the US), thus, no reasonably supported statistics aside from anecdotal information and surveys.

37. What is equally as important is establishing a right of action for third parties. Individual users often lack the technical expertise and financial resources to take action against spammers and other cyber criminals. A third party right of action could protect consumers, which could include our own customers, by bringing damage claims that deter cyber criminals from continuing their activities. Companies could also recover some of the economic losses that cybercriminals cause to them in increased security costs and reputational damage.

38. We have developed strong partnerships with Interpol, other law enforcement agencies, government and industry to tackle the problems of online crime.

39. Earlier this year we launched our Global Phishing Enforcement Initiative (GPEI), which focuses on the identification and prosecution of individuals and groups involved with online phishing attacks. We have identified 104 phishing sites in 39 European countries. Of these sites, 31 are in English. We have initiated 53 separate legal actions. Of these actions, 4 are in the UK. The majority of phishers are males aged between 16 and 20. Legal actions include: criminal complaints, civil lawsuits, court orders and settlements. The four major offenders are: Spain, France the UK and the Netherlands.

Conclusion

40. It would aid consumer understanding and more consistent evidence collecting and tracking of the scale and growth of the problem if the topics were more consistently described. For example, we recommend that the phrase "identity fraud" be defined more clearly and consistently. At present, much so-called "identity fraud" can often actually be related to other issues—such as benefit claimants misrepresenting their circumstances.

41. We also believe it is worth considering the establishment of a UK-wide, simple streamlined system for reporting of all cyber crime and online problems such as phishing. This would enable much easier reporting by citizens and hence much better insight and analysis of the true scale of the problem. Ensure that law and enforcement agencies are appropriately resourced to track, monitor and tackle cyber crime and related identity fraud.

42. Both the offline world and online, digital world lack a clear identity layer. We need to work collectively to establish a clear policy framework for identity. We recommend the "Laws of Identity" (Annex A) as a starting point.

43. Microsoft believes criminal enforcement against those undertaking identity theft and related fraud, including for example, phishers is important to ensure that cyber criminals understand there will be consequences to illegal actions. In particular, establishing a right of action for third parties.

44. The UK should ensure it has not only the necessary legislation itself, but given the international nature of Internet threats, work with other countries to ensure reciprocal arrangements are in place to curtail the way in which criminals currently use international boundaries to impede the process of criminal proceedings.

45. It is also important the law enforcement agencies are provided with sufficient investment in their forensic analysis capability to tackle Internet-based crime.

46. The evolution of the computing ecosystem and malicious software threat landscape requires continual re-thinking about how to make consumer computing environments more secure. 64-bit computing is already making an impact as the next significant PC computing architecture. To support this new architecture (and to create an ecosystem that engenders trust and accountability), the security industry must continue to innovate on the development of more secure solutions.

47. At Microsoft, we know we can't do this alone and are committed to working with partners on ways to enhance our platform and provide greater opportunity for all software providers to build new solutions for consumers.

Annex A

THE LAWS OF IDENTITY

1. User Control and Consent

Technical identity systems must only reveal information identifying a user with the user's consent.

No one is as pivotal to the success of the identity metasystem as the individual who uses it. The system must first of all appeal by means of convenience and simplicity. But to endure, it must earn the user's trust above all.

Earning this trust requires a holistic commitment. The system must be designed to put the user in control—of what digital identities are used, and what information is released.

The system must also protect the user against deception, verifying the identity of any parties who ask for information. Should the user decide to supply identity information, there must be no doubt that it goes to the right place. And the system needs mechanisms to make the user aware of the purposes for which any information is being collected.

The system must inform the user when he or she has selected an identity provider able to track internet behavior.

Further, it must reinforce the sense that the user is in control regardless of context, rather than arbitrarily altering its contract with the user. This means being able to support user consent in enterprise as well as consumer environments. It is essential to retain the paradigm of consent even when refusal might break a company's conditions of employment. This serves both to inform the employee and indemnify the employer.

The Law of User Control and Consent allows for the use of mechanisms whereby the metasystem remembers user decisions, and users may opt to have them applied automatically on subsequent occasions.

2. Minimal Disclosure for a Constrained Use

The solution which discloses the least amount of identifying information and best limits its use is the most stable long term solution.

We should build systems that employ identifying information on the basis that a breach is always possible. Such a breach represents a risk. To mitigate risk, it is best to acquire information only on a "need to know" basis, and to retain it only on a "need to retain" basis. By following these practices, we can ensure the least possible damage in the event of a breach.

At the same time, the value of identifying information decreases as the amount decreases. A system built with the principles of information minimalism is therefore a less attractive target for identity theft, reducing risk even further.

By limiting use to an explicit scenario (in conjunction with the use policy described in the law of control), the effectiveness of the "need to know" principle in reducing risk is further magnified. There is no longer the possibility of collecting and keeping information "just in case" it might one day be required.

The concept of "least identifying information" should be taken as meaning not only the fewest number of claims, but the information least likely to identify a given individual across multiple contexts. For example, if a scenario requires proof of being a certain age, then it is better to acquire and store the age category rather than the birth date. Date of birth is more likely, in association with other claims, to uniquely identify a subject, and so represents "more identifying information" which should be avoided if it is not needed.

In the same way, unique identifiers that can be reused in other contexts (for example drivers' license numbers, social security numbers and the like) represent "more identifying information" than unique special-purpose identifiers that do not cross context. In this sense, acquiring and storing a social security number represents a much greater risk than assigning a randomly generated student or employee number.

Numerous identity catastrophes have occurred where this law has been broken. We can also express the Law of Minimal Disclosure this way: aggregation of identifying information also aggregates risk. To minimise risk, minimise aggregation.

3. Justifiable Parties

Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.

The identity system must make its user aware of the party or parties with whom they are interacting while sharing information.

The justification requirements apply both to the subject who is disclosing information and the relying party who depends on it. Our experience with Microsoft's Passport is instructive in this regard. Internet users saw Passport as a convenient way to gain access to MSN sites, and those sites were happy using Passport—to the tune of over a billion interactions per day. However, it did not make sense to most non-MSN sites for Microsoft to be involved in their customer relationships. Nor were users clamoring for a single Microsoft identity service to be aware of all their Internet activities. As a result, Passport failed in its mission of being an identity system for the Internet.

We will see many more examples of this law going forward. Today some governments are thinking of operating digital identity services. It makes sense (and is clearly justifiable) for people to use government-issued identities when doing business with the government. But it will be a cultural matter whether, for example, citizens agree it is "necessary and justifiable" for government identities to be used in controlling access to a family wiki—or connecting a consumer to their hobby or vice.

The same issues will confront intermediaries building a trust fabric. The law is not intended to suggest limitations of what is possible, but rather to outline the dynamics of which we must be aware.

We know from the law of control and consent that the system must be predictable and "translucent" in order to earn trust. But the user needs to understand who they are dealing with for other reasons, as we will see in law six (human integration). In the physical world we are able to judge a situation and decide what we want to disclose about ourselves. This has its analogy in digital justifiable parties.

Every party to disclosure must provide the disclosing party with a policy statement about information use. This policy should govern what happens to disclosed information. One can view this policy as defining "delegated rights" issued by the disclosing party.

Any use policy would allow all parties to co-operate with authorities in the case of criminal investigations. But this does not mean the state is party to the identity relationship. Of course, this should be made explicit in the policy under which information is shared.

4. Directed Identity

A universal identity system must support both "omni-directional" identifiers for use by public entities and "unidirectional" identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.

Technical identity is always asserted with respect to some other identity or set of identities. To make an analogy with the physical world, we can say identity has direction, not just magnitude. One special "set of identities" is that of all other identities (the public). Other important sets exist (for example, the identities in an enterprise, some arbitrary domain, or in a peer group).

Entities that are public can have identifiers that are invariant and well-known. These public identifiers can be thought of as beacons—emitting identity to anyone who shows up. And beacons are "omni directional" (they are willing to reveal their existence to the set of all other identities).

A corporate web site with a well-known URL and public key certificate is a good example of such a public entity. There is no advantage—in fact there is a great disadvantage—in changing a public URL. It is fine for every visitor to the site to examine the public key certificate. It is equally acceptable for everyone to know the site is there: its existence is public.

A second example of such a public entity is a publicly visible device like a video projector. The device sits in a conference room in an enterprise. Visitors to the conference room can see the projector and it offers digital services by advertising itself to those who come near it. In the thinking outlined here, it has an omni-directional identity.

On the other hand, a consumer visiting a corporate web site is able to use the identity beacon of that site to decide whether they want to establish a relationship with it. Their system can then set up a "unidirectional" identity relation with the site by selecting an identifier for use with that site and no other. A unidirectional identity relation with a different site would involve fabricating a completely unrelated identifier. Because of

this, there is no correlation handle emitted that can be shared between sites to assemble profile activities and preferences into super-dossiers.

When a computer user enters a conference room equipped with the projector described above, its omni-directional identity beacon could be utilized to decide (as per the law of control) whether they want to interact with it. If they do, a short-lived unidirectional identity relation could be established between the computer and the projector—providing a secure connection while divulging the least possible identifying information in accordance with the law of minimal disclosure.

Bluetooth and other wireless technologies have not so far conformed to the fourth law. They use public beacons for private entities. This explains the consumer backlash innovators in these areas are currently wrestling with.

Public key certificates have the same problem when used to identify individuals in contexts where privacy is an issue. It may be more than coincidental that certificates have so far been widely used when in conformance with this law (ie in identifying public web sites) and generally ignored when it comes to identifying private individuals.

Another example involves the proposed usage of RFID technology in passports and student tracking applications. RFID devices currently emit an omni-directional public beacon. This is not appropriate for use by private individuals.

Passport readers are public devices and therefore should employ an omni-directional beacon. But passports should only respond to trusted readers. They should not be emitting signals to any eavesdropper which identify their bearers and peg them as nationals of a given country. Examples have been given of unmanned devices which could be detonated by these beacons. In California we are already seeing the first legislative measures being taken to correct abuse of identity directionality. It shows a failure of vision among technologists that legislators understand these issues before we do.

5. Pluralism of Operators and Technologies:

A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers.

It would be nice if there were one way to express identity. But the numerous contexts in which identity is required won't allow it.

One reason there will never be a single, centralized monolithic system (the opposite of a metasystem) is because the characteristics that would make any system ideal in one context will disqualify it in another.

It makes sense to employ a government issued digital identity when interacting with government services (a single overall identity neither implies nor prevents correlation of identifiers between individual government departments), but in many cultures, employers and employees would not feel comfortable using government identifiers to log in at work. A government identifier might be used to convey taxation information; it might even be required when a person is first offered employment. But the context of employment is sufficiently autonomous that it warrants its own identity, free from daily observation via a government-run technology.

Customers and individuals browsing the web meanwhile will in many cases want higher levels of privacy than is likely to be provided by any employer.

So when it comes to digital identity, it is not only a matter of having identity providers run by different parties (including individuals themselves), but of having identity systems that offer different (and potentially contradictory) features.

A universal system must embrace differentiation, while recognizing that each of us is simultaneously—in different contexts—a citizen, an employee, a customer, a virtual persona.

This demonstrates, from yet another angle, that different identity systems must exist in a metasystem. It implies we need a simple encapsulating protocol (a way of agreeing on and transporting things). We also need a way to surface information through a unified user experience that allows individuals and organizations to select appropriate identity providers and features as they go about their daily activities.

The universal identity metasystem must not be another monolith. It must be polycentric (federation implies this) and also polymorphic (existing in different forms). This will allow the identity ecology to emerge, evolve and self-organise. Systems like RSS and HTML are powerful because they vehicle any content. We need to see that identity itself will have several—perhaps many—contents, and yet can be expressed in a metasystem.

6. Human Integration:

The universal identity metasystem must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks.

We have done a pretty good job of securing the channel between web servers and browsers through the use of cryptography—a channel that might extend for thousands of miles. But we have failed to adequately protect the two or three foot channel between the browser's display and the brain of the human who uses it. This immeasurably shorter channel is the one under attack from phishers and pharmers. No wonder. What identities is the user dealing with as they navigate the web? How understandably is identity information conveyed to them? Do our digital identity systems interface with users in ways that objective studies have shown to work? Identity information currently takes the form of certificates. Do studies show certificates are meaningful to users?

What exactly are we doing? Whatever it is, we've got to do it better: the identity system must extend to and integrate the human user.

Carl Ellison and his colleagues have coined the term "ceremony" to describe interactions that span a mixed network of human and cybernetic system components—the full channel from web server to human brain. A ceremony goes beyond cyber protocols to ensure the integrity of communication with the user. This concept calls for profoundly changing the user's experience so it becomes predictable and unambiguous enough to allow for informed decisions.

Since the identity system has to work on all platforms, it must be safe on all platforms. The properties that lead to its safety can't be based on obscurity or the fact that the underlying platform or software is unknown or has a small adoption.

One example is United Airlines' Channel 9. It carries a live conversation between the cockpit of one's plane and air traffic control. The conversation on this channel is very important, technical and focused. Participants don't "chat"—all parties know precisely what to expect from the tower and the airplane. As a result, even though there is a lot of radio noise and static, it is easy for the pilot and controller to pick out the exact content of the communication. When things go wrong, the broken predictability of the channel marks the urgency of the situation and draws upon every human faculty to understand and respond to the danger. The limited semiotics of the channel mean there is very high reliability in communications.

We require the same kind of bounded and highly predictable ceremony for the exchange of identity information. A ceremony is not a "whatever feels good" sort of thing. It is predetermined.

But isn't this limitation of possibilities at odds with our ideas about computing? Haven't many advances in computing come about through ambiguity and unintended consequences which would be ruled out in the austere light of ceremony?

These are valid questions. But we definitely don't want unintended consequences when figuring out who we are talking to or what personal identification information to reveal.

The question is how to achieve very high levels of reliability in the communication between the system and its human users. In large part, this can be measured objectively through user testing.

7. Consistent Experience Across Contexts

The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.

Let's project ourselves into a future where we have a number of contextual identity choices. For example:

- browsing: a self-asserted identity for exploring the web (giving away no real data);
- personal: a self-asserted identity for sites with which I want an ongoing but private relationship (including my name and a long-term email address);
- community: a public identity for collaborating with others;
- professional: a public identity for collaborating issued by my employer;
- credit card: an identity issued by my financial institution;
- citizen: an identity issued by my government.

We can expect that different individuals will have different combinations of these digital identities, as well as others.

To make this possible, we must "thingify" digital identities—make them into "things" the user can see on the desktop, add and delete, select and share. How usable would today's computers be had we not invented icons and lists that consistently represent folders and documents? We must do the same with digital identities.

What type of digital identity is acceptable in a given context? The properties of potential candidates will be specified by the web service from which a user wants to obtain a service. Matching thingified digital identities can then be displayed to the user, who can select between them and use them to understand what information is being requested. This allows the user to control what is released.

Different relying parties will require different kinds of digital identities. And two things are clear:

— a single relying party will often want to accept more than one kind of identity; and

— a user will want to understand his or her options and select the best identity for the context.

Putting all the laws together, we can see that the request, selection, and proffering of identity information must be done such that the channel between the parties is safe. The user experience must also prevent ambiguity in the user's consent, and understanding of the parties involved and their proposed uses. These options need to be consistent and clear. Consistency across contexts is required for this to be done in a way that communicates unambiguously with the human system components.

As users, we need to see our various identities as part of an integrated world which none the less respects our need for independent contexts.

Examination of Witnesses

Witnesses: Mr Jerry Fishenden, National Technology Officer, and Mr Matt Lambert, Government Affairs Director, Microsoft UK, examined.

Q261 ***Chairman:*** Mr Fishenden and Mr Lambert, thank you very much for coming to join us. Welcome to members of the public who are here for this evidence session. First I would like you to introduce yourselves and then if you wish you can make an opening statement or we will go straight into the questions.
Mr Fishenden: Thank you Chairman. I am Jerry Fishenden. I am National Technology Officer for Microsoft here in the UK.
Mr Lambert: I am Matt Lambert. I am Director of Government Affairs for Microsoft also in the UK.

Q262 ***Chairman:*** Would you like to make a statement at the beginning?
Mr Fishenden: I would like to make a few brief opening comments if I may to reiterate some of the points we made in our written submission in that we see successful combating of cyber crime and criminal activity on-line as comprising three core components, not just the technology. We look at consumer or citizen education, making sure that people are much more aware of the threats they face when they are on-line and how they can mitigate those. The technology itself, of course, is constantly changing and evolving as time goes by and a lot of tools will be provided to users to help them visibly protect their PC when on-line. They range from things like anti-phishing filters to identify if you are going to a rogue website to anti-malware that tries to prevent spyware and the like being installed on your machine. The third part is the enforcement, which is making sure that we are working collectively on prosecuting cyber criminals, if you want to call them that, criminals who are making use of the Internet and PCs and the like, so that there are deterrents to them and people know they will be investigated and prosecuted as appropriate.

Q263 ***Chairman:*** Do you wish to add anything, Mr Lambert?
Mr Lambert: No.

Q264 ***Chairman:*** Let me start with the first question. Who do you believe should be responsible for keeping end user machines secure?
Mr Fishenden: If we go back to the preceding comments about the three-way relationship, I think it is a collective responsibility. I certainly think consumers themselves need to be aware of some of the issues that they face, if you take something like phishing, where people are perhaps receiving fraudulent emails claiming to be from their bank, that they understand how they might identify those if they have managed to get through to them, or that when they go to a website they look for any visual cues there might be that that is not really their bank but perhaps a site that some fraudulent people have set up who are trying to get hold of their identity information and perpetrate some fraud against them. You can see that making sure that users themselves are aware is a core component. There is a lot of work in the UK specifically with things like Get Safe Online, an initiative which is a mixture of private and public sector initiatives. There is a lot of context relevant information that we provide in our tools and other companies do in theirs so that people are as aware as we can make them of some of the risks and the types of things they need to be thinking about themselves. The second part is the technology itself.

That continues to evolve. Every time the bad guys, if you like, move their attacks onto new elements of the Internet ecosystem the industry moves on as well and begins to provide more tools to lock down and protect the PC environment for users to try and make sure that they are as secure as they possibly can be without taking away from the users the very benefits that the Internet is meant to bring. Obviously, you can go to extremes if you lock down a PC so that it is so secure that it becomes almost unusable to the user, so there is a balance to be struck between what the technology can do and how the user interacts with that. On the legal side we have taken legal action. Just under a year ago I helped launch in the UK our Global Phishing Enforcement Initiative. We have taken a number of people to court around the European area, prosecuting them where they have, for example, set up a fake Microsoft site, so pretending to be a Microsoft site, asking people to log in with their user ID details and then misappropriating them and using them for illegal purposes. If all three of those are being worked on collectively we see that as the most effective way of making sure that users have the most secure experience when they are on-line.

Q265 ***Chairman:*** Does Microsoft accept ultimate liability for the security of machines running its software, and, if not, how do you engage with retailers, security practitioners and end users in keeping machines secure?
Mr Fishenden: We provide a range of tools, as I have mentioned, anti-phishing and anti-malware, and a variety of our partners do as well, and users are free to choose whether they want to use Symantec or Norton or any of the other tools that are out there and we make sure our platform offers that choice to users. In terms of whether the user decides to use them, that is obviously their choice. We always recommend that they do, that they look to protect themselves as best they can. There are issues that occasionally come up. If you take the example of parental controls, which attempt to secure the on-line environment for younger children in the household, sometimes if they are not configured properly people find that they become so intrusive into their Internet experience that they end up switching them off, which obviously is not desirable but there is an interesting trade-off, if you like, sometimes between security that people want to put into place and the practical experience of using some of those tools and how intrusive they can be into people's daily experience of the Internet.

Q266 ***Lord O'Neill of Clackmannan:*** With regard to the tools that are incorporated in the next generation of Microsoft Windows, to what extent are those reflected in the increased cost of the next generation of Windows? Is cost a factor? Is it reflected in price or is it absorbed by you?
Mr Fishenden: For each generation of software we release to market substantial research and development goes into it. Typically each year we are spending something like seven to eight billion dollars on R&D. Generally when we bring a new product to market it is priced in accordance with the investment that we have put into it. To be honest, I am not a licensing person. I am not precisely sure what the formally announced list price is in the UK. Generally upgrade prices are already in place on pre-installed machines such as Dell and Compaq, and the others are reasonably consistent from one generation of Windows to the next. People have the choice of staying with their existing operating system and existing Windows applications or they can decide that there is sufficient reason why they would want to move to something like Windows Vista. Obviously, we think there are good reasons why you would want to move, and not just for security. There are many other features in Vista that perhaps are not relevant to today's inquiry, but we exist in a market place. People vote with their feet. They can see different parts of the market. People make different decisions. We have made available media players for years and Apple comes along and does a very good job with the iPod, for example, in that particular market. Consumers are very quick to decide whether what any of us offer in the market place is a product that they want to choose to adopt or not.

Q267 ***Lord O'Neill of Clackmannan:*** If I were going, as I was a few weeks ago, to get a new computer for our house and I was incorporating the latest Windows into that, would you make available to salesmen the kind of information that I have just asked you: how much more am I paying this time than the last and how much of that is accounted for by additional security? I accept that it is required but I think one is always a wee bit curious, given your market dominance, as to the extent to which you might be exploiting your market dominance when you are selling additional products.
Mr Lambert: I think, Lord O'Neill, that there is not a huge difference, if any, in the price increase between XP and Vista. The honest answer to your question is that I do not think the salesperson in PC World or Dixons is going to be able to answer that question. It is not an easy question to answer, but I think overall the answer is that the cost of these improvements is absorbed over time and the cost does indeed, as Jerry Fishenden has already said, reflect the huge cost in research and development that goes on over a number of years, as he said, about seven billion dollars a year.

Q268 ***Baroness Sharp of Guildford:*** Can you tell us how far these tools are available as updates for those who do not shift from one operating system to another? For example, I updated my computer about 18 months ago and I am on XP and would not expect to update probably for another 18 months on my home computer. Does the updating that I download automatically from Microsoft include these anti-phishing tools and so forth?
Mr Fishenden: Yes, it does. Windows XP is fully capable of downloading the anti-phishing tools, anti-malware detection and removal tools and the like. The new version of Internet Explorer is available as well, which has anti-phishing tools in it, and there are other facilities to help users. There are one or two minor differences between the way those tools work in Windows Vista and in Windows XP because of the new security features, but you as a Windows XP user can get the vast majority of those components freely downloadable from the Microsoft update site.

Q269 ***Chairman:*** Overall would you say that Microsoft software is secure?
Mr Fishenden: It is part of a complex eco-system. I think any piece of software is inherently a complex product that is designed to be very configurable by the end user. They can choose how they want to use it in many different types of environment and situation. They can add on many different thousands of third party hardware devices and many thousands of different applications that people make available. We are doing the best that we can to make sure that the core platform of tools that we ship to users is as secure as we can possibly make it. Over time, of course, we will continue to get feedback and information from police and other agencies about the way people might be trying to exploit the platform. We ourselves monitor the way that people might be trying to attack our platform and its applications, and we learn from that and try to make available back to our users products that then address the issues that we have highlighted.

Q270 ***Chairman:*** Some open source software, such as Red Hat Linux, is shipped with built-in firewall protection, and that has been the case for years, I believe. Why is Microsoft only now following this route?
Mr Fishenden: We seem to be between a rock and a hard place with this. If we slowly extend our platform and put more and more features in it to help our users, some of our competitors say, "That is a core business that we were building up". There have always been third party firewall providers for the Windows platform and many of those companies have made very successful businesses out of it. We took a decision as of Windows XP SP2 to build some core firewall functionality into those products because we were aware, based on the information we get back from the police and other people, of the types of attack being made on this platform and we wanted to make sure that at least the core shell, if you like, of Windows was as secure as it could be, but we have been very cognisant of the fact that there are third party companies making their own products that they want to sell in the market place to Windows users and that we need to design the platform in such a way that end users can choose to push off those features we provide and enable their choice of firewall or other software, such as anti-phishing software.

Q271 ***Lord Harris of Haringey:*** But until about two and a half years ago the firewall default was switched off.
Mr Fishenden: Yes, that is true.

Q272 ***Lord Harris of Haringey:*** Why?
Mr Fishenden: A lot of this goes back to usability. Over time we have moved more to the default position of putting security on, partly as people have become more educated. There is an issue, and it is the parental controls example earlier on, whereby when you try and lock down certain features of the platform people do have to have a better understanding of the way the software works. Typically I can see that when I am talking to my neighbours about the types of issues they have, say, in setting up wireless networks. You begin to understand some of the issues because if people need to go and open up ports on their firewalls to get certain things to work there are issues of user education, which is why I made the earlier point that there is quite a careful balance between the tools we make available and the defaults we put on those and the consumer understanding then how they can use that platform securely when they are trying to access the Internet and set up a home network or maybe share files between different PCs in their home environment.

Q273 ***Lord Mitchell:*** Is the practice of selling software "as is", warts and all, still an acceptable practice? Should you not be making your software much more fit for purpose and taking legal responsibility for the damage your security holes cause?
Mr Fishenden: I would contend that we are making our platform as secure as we possibly can within the complex nature of software. Our third party partners are working with us as well, so if you take the example of Windows Vista, we have been working for over two years now with third party anti-virus providers and the like so that we can provide users with as secure an experience as is humanly possible with these very complex pieces of software. There is a broader issue. By analogy you talk about the physical

world. People do not tend to immediately look for liability towards lock or window companies because houses are still being burgled. The tendency is to want to blame the perpetrator rather than the people who are the victims of those types of assault. When you look at software, which is inherently more complex than a lot of the physical world, I do not really see why the same example would not apply whereby you would be after the perpetrator.

Q274 ***Lord Mitchell:*** How do you measure security? You say things are getting better. How do you internally measure security?
Mr Fishenden: Five years ago we adopted something known as the Trustworthy Computing Initiative which took a lot of people out of development, about 8,500 developers in the US, in order to look through very specific secure coding programmes, and the true measure of what we have achieved is in the statistics of monitoring the number of vulnerabilities on our platform over time and by specific product over time compared to earlier products. There has been a dramatic reduction in the number of security vulnerabilities on our platform which to us is a reflection of the progress we have made under the Trustworthy Computing Initiative. Of course, there is always progress to be made. Every time we tackle a particular security issue or vulnerability the hackers out there and other people are constantly moving forward and finding new ways of attacking the platform.

Q275 ***Lord Mitchell:*** I suspect I know how you are going to answer this question but I will ask it all the same. Is it fair to say that Microsoft has been more concerned with establishing market dominance by rushing out operating systems than they are with ensuring that their security and fitness for purpose exists?
Mr Fishenden: I guess I would almost take the opposite view. We have been waiting five years for Windows Vista. I certainly do not think it is true that we have been rushing out new operating systems without due account of security. In fact, one of the reasons it was delayed was that, when we took all of those people out of developing new products such as Vista and put them through a rigorous training exercise on the secure codes, we then released a pretty major update to Windows XP, which was mentioned before, a service pack which was deliberately designed to put in a lot of additional security features and that included things like the firewall being on by default. There is a lot of debate about that in the industry, about whether it should be on or off by default. I think we have shown due diligence, if you like, and have not just been stampeding endlessly towards new operating systems and getting them out of the door before they are ready. I think we have paid a lot of attention to our existing users, trying to make sure they are happy with the existing gear, and that Windows Vista, when it comes out, is the most secure operating system we have.

Q276 ***Lord Howie of Troon:*** Microsoft has been in dispute with the European Commission for some time on anti-competitive grounds, and last year made changes to the Vista operating system which was alleged might have prevented competitors' security software from running. There has to be a balance struck between security and open competition. Where do you think that should be?
Mr Lambert: I think there has to be essentially a balance there and, as Mr Fishenden has already said, we believe that Windows Vista is the most secure version of our operating systems that we have ever produced, but within that you have to accept that consumers have to be given an absolute choice to load whatever other security software they want to put onto their system and that manufacturers of PCs and hardware can also ship PCs loaded with Vista with other people's security software pre-loaded on it when the consumer buys the PC for the first time. That is a critical principle that we have accepted all the way along and have always tried to build into our operating systems. One of the things about Windows is that we work with manufacturers and all sorts of other software applications to try and give them as much information in advance as we can so that they can build good applications ready for when, for example, Vista launches to the public market in a few days' time so that they are ready to go with some of those software applications that are sold with new PCs as they go out of the door after the launch at the end of January. That was the approach that we took and when we were sitting down with the Commission, as you rightly say, we were discussing a number of these issues and we have been in dispute with DG Competition at the European Commission for a number of years in a case that will be resolved when the Court of First Instance gives us a judgment some time later this year, we think, to our appeal against the ruling from the European Commission. When we look at a new system what we want to do is move beyond that. We do not want to spend more of our time arguing with competitors and competition authorities. We try to work with them as closely as we can and listen to what they are saying, and we try to respond to that within the grounds of producing products which our consumers find in this case safe and secure. What we did there was that we sat down with the Commission and said, "What is the nature of these complaints?", and there were a couple of areas that came up, some of which were nothing to do with security, but on security we listened to what they said and we produced a number of what we call APIs, application programme interfaces, which we shared

with any of our competitors so that they can work with our system and produce their security products effectively with Vista and satisfy their concerns. We are very happy to do that. What we are trying to do is move into an area where it is more a matter of discussion and agreement rather than sitting before judges in Luxembourg trying to debate the ins and outs of our different efforts to comply with the law. That is where we stand. I think some what the consumer is getting is the best of both worlds. They are getting Windows Vista with the most secure operating system that has ever been available, plus they are absolutely free to choose anybody else's security software which will work, we hope, very well with Windows. It is designed to work well with Windows, and we work with them to make sure that it does. For example, one of the areas which was a matter for debate was the Windows Security Center. The Windows Security Center, as I say, is essentially a dashboard at which you can check which security software is running on your operating system on your PC. Some of our competitors were concerned about whether that would potentially favour some of our security software. In fact it does not; it is absolutely neutral, and what the Security Center does is just tell you if there is a problem with somebody else's software security or with ours, so you can see immediately if there is any issue there and resolve it. That is essentially what we are trying to do, that is, all the time build a neutral operating system which others can work with very easily and consumers can get a good deal on in terms of the Microsoft software that they are using and other people's software on our system.

Q277 ***Lord Howie of Troon:*** That was a very full reply. Do you feel that you have met the Commission's concerns?
Mr Lambert: We believe that we have. The Commission always has a right to make its own view known on that and come to its own conclusions and, if it does not feel that we have done that then it will, I am sure, tell us. What we are trying to do, as I said earlier, with the Commission is work with them on a basis of co-operation so that, rather than going back before the courts, we would ask them, "If you do have concerns about this, what we have done, or other things that you might want us to do, come and tell us". We are in a process of constant dialogue with the Commission anyway. If they tell us we will listen and if the objections or requests are reasonable we will do our best to comply with them.

Q278 ***Lord Howie of Troon:*** Why has the dispute gone on so long?
Mr Lambert: You are probably aware that the legal process in Europe, when you are going before the Court of First Instance, just takes a very long time. These are very complex issues, so when you are discussing them with the Commission experts are poring over them, sometimes other competitors or interested parties are raising issues. These are all complex matters. There have to be public hearings sometimes. It does take a long time. There is some frustration on our part. We have been before the legal process in Europe for eight years now. It is a distraction and one would hope that in an ideal world it could be settled out of court much more quickly than that.

Q279 ***Lord Howie of Troon:*** So none of the delay was your fault?
Mr Lambert: I contend that we have tried to comply with everything that was asked of us in terms of supplying information as quickly as possible, but it is a fact that if you take an appeal to the Court of First Instance it takes a long time. We gave evidence at a hearing back in April. We are still waiting for the judgment from the Court of First Instance. These are complex matters. The judges have to look into them very carefully and it takes a long time.

Q280 ***Earl of Erroll:*** Presumably there is a logical problem that if your Security Center is sitting there making sure that malware is not appearing to be an anti-virus programme you have to run a second level of security all the time even though someone has bought yet another virus checker, or otherwise your system will become insecure. Therefore, to a large extent an extra virus checker must always logically be redundant if you have a totally secure system.
Mr Lambert: You can have an extra virus checker but you can switch off the Windows Security Center if you really do not want that running on your system. It is very easy just to switch it off.

Q281 ***Earl of Erroll:*** But then presumably your system would be vulnerable because someone can then use your API to write malware to access the computer?
Mr Lambert: Jerry may want to comment but I would say that that is up to the consumer which kind of system they use to check on what is operating and how it is operating. If they do not want to use the Windows version they do not have to.

Q282 ***Earl of Erroll:*** What I am saying is that I suppose that anti-competition law here is actually militating against being able to write a more secure system. There is a conflict there.
Mr Lambert: You could say that. I do not wish to make that comment.

Q283 ***Lord Harris of Haringey:*** Can I just make sure I have understood your earlier answers? What you seem to be saying is that you have no problem at all in

terms of making your software compatible with other people's security software, and in essence you would have done this if you had been asked without the intervention of the European Commission.
Mr Lambert: We have always worked with other companies, including competitors, to try to make our systems as inter-operable as possible. That is a cross-industry issue because it takes two to tango essentially. We believe and we have always believed, and this is one of the cornerstones of our appeal in the European case, that we have made the information available to allow our competitors to work with our software and that we do that with partners and competitors alike. We make these application programme interfaces widely available. There are constantly conferences with developers, small businesses and large businesses alike, explaining to them what we are doing, what we are developing. Even in the development stage of Vista we did that so that people know what is coming and they can work with our systems.

Q284 ***Lord Harris of Haringey:*** But changes were made in response to the European Commission?
Mr Lambert: They were indeed.

Q285 ***Lord Harris of Haringey:*** So why, if you were so ready to co-operate, was it necessary to have the intervention by the European Commission to make those changes, or are you saying those changes are irrelevant?
Mr Lambert: When you are developing software others have different opinions. That is the same with anything in life. If others come to us and say, "We have looked at what you have offered here. We do not find it easy to inter-operate". This is one of the contentions of some of our competitors and in some part of the Commission. You do your best to comply with that. There are some points at which you say, "What you are asking is not acceptable. We cannot go down that road". Sometimes there have been points like that in the discussions in the case with the European Commission, but on the whole we start from the point of view that we try to make Windows a system that inter-operates well with other people's software. It is in our interests to do that. We are not, as Jerry Fishenden has said, trying to produce software for every single possible eventuality. We are trying to produce an operating system which meets consumers' needs and which allows other businesses to operate on it. There are huge numbers of businesses here in the United Kingdom, 17,000 partners in Britain alone producing software which works on our platform.

Q286 ***Lord Harris of Haringey:*** But the implication of what you are saying is that there were changes that you have made to Vista software which were unacceptable to you, and you have only made them in response to the European Commission.
Mr Lambert: There are some things that we did that perhaps we took longer to negotiate than others, and eventually, of course, as you know, we are appealing the ruling because we believe that companies like our own should have the right to innovate and build new things into Windows in response to consumer demand. The world does not stand still and only one version of Windows will ever hold. That is a product which is constantly developing and responding to consumer demand and changes in the market but there are some things which the Commission have asked of us that were reasonable and some things that we were able to do that we were happy to do. There are two types of issue there.

Q287 ***Lord Harris of Haringey:*** But there were by implication some things that you were not happy with having to do?
Mr Lambert: There are some things that we have done which are matters of dispute. For example, we are on record as being in dispute. One of the things that we have appealed against is a request from the Commission, which we complied with, in which we produced a version of Windows, in the last version of Windows, called Windows N which does not have a media player in it. The Commission contested that there was a market for an operating system for Microsoft without a media player in it and if you produced that it would help competitors produce other media players to get their products more widely into the market here and in Europe, and so for the European market we have produced Windows N. It has not sold very many copies and we have sold in the meantime many millions of versions of ordinary Windows because it works better, it is at the same price and it has a media player. We believe that consumers expect a media player to be in an operating system. It is in all the other operating systems. That is just one example.

Q288 ***Earl of Erroll:*** Large corporations can download security patches and test them before implementing them on their main systems. Ordinary users do not have that ability, so how can they be certain that they are downloading the patches from the genuine Microsoft site, they are not being tampered with by some existing malware on their system and that they are going to make things better and not cause some other things to malfunction?
Mr Fishenden: There is obviously a key difference between a business environment and a home environment. A business environment usually has a test environment where they cream out—

Q289 ***Earl of Erroll:*** Small businesses are very often in a home-type environment, a small business office, someone with five or 10 employees. There are about three and a half million employees in this country employed by micro businesses.
Mr Fishenden: Yes, sure, I accept that entirely. If we look at the way the Microsoft update facility works for those users and any home users, people have the option of entirely opting in, which we recommend and which is where an update is published on the official Microsoft update site. It not only identifies the patch that is available; it also downloads it and installs it for you, and that is the recommended option. Users then have the choice of other options. They can say, "Notify me it is there but do not do anything else", or they can say, "Download it but do not install it because I want to see what is in it and whether it is appropriate for me to install or not", because they might be patching something that users have chosen to disable on that particular PC. We believe that offers pretty good flexibility. The other option I should mention is that they can switch it off entirely and not patch anything should they so choose, which is not recommended but that is up to them. The way the Microsoft update environment works in the operating system is that it communicates only with our professional designated distribution points, so you know that the update is coming from an accredited source and has not been tampered with. There have been occasions in the past where people have taken some of our updates and attempted to distribute them via other mechanisms, and people often ask why we stopped that. It is because, Chairman, it is precisely the type of issue you are raising in that how can you guarantee complete assurance that that software, once it is downloaded, is not tampered with, in the same way that some pirated copies of Windows are tampered with and do come pre-installed with malware and spyware and the like. If you do not get things from a legitimate source I think your concern is a well justified one, that you may in fact be running the risk of installing software that we cannot be entirely sure is as trustworthy as you think it might be.

Q290 ***Earl of Erroll:*** Have you had problems though with patches not behaving as they should on home computers?
Mr Fishenden: On occasion that has happened with a few. We do put them through a very extensive testing programme. Typically where that has happened will be with maybe a specific third party hardware driver or something where there is some conflict. Despite the many thousands of permutations that we run in America, and we have huge test labs where we run as many mainly third party pieces of hardware or software as we possibly can, there have occasionally been a couple of incidents, I believe, where there were issues on a small number of machines when a patch was not deployed. We then run a fairly rapid escalation process to try and understand why a patch has worked on the vast majority of machines but is having an issue on some. Sometimes it could be that those are machines where some malware has replaced something that our patches cannot fix and it is a problem because it does not find the file it was expecting and, as I say, maybe produces some sort of third party device driver conflict where we then need to identify the particular provider of that and work with them so that we can collectively solve the problem.

Q291 ***Earl of Erroll:*** Of course, the trouble then is that if this does happen to someone they then lose confidence in doing patches because if they lose their Internet connectivity they cannot then cure the problem or it is very difficult to do so.
Mr Fishenden: The patches are reversible, so you can go back into the installed programmes menu, find "Patches" and roll back. If you are not able to do it by underscoring that patch there are quite a lot of facilities in the platforms as well now called "Rollback", because you can roll back to the previously known good state. If you imagine a hypothetical situation where you download some updates and that is creating some sort of behaviour on the PC which means it is unusable, you can then elect to roll back to the previous state that PC was in before the update was applied, and then you can contact us and say, "Look: I had a problem when I applied this and I have had to roll back", and we try and find out what the issue is.

Q292 ***Earl of Erroll:*** You roll out your patches on the second Tuesday of each month. This, of course, is timetabled to suit you and business but do you find that being exploited by malware writers because there is a window of opportunity for them then before systems get patched?
Mr Fishenden: On occasions where we believe there has been a live risk to people of significant proportions then we have occasionally slipstreamed updates between the regular monthly schedules.

Q293 ***Earl of Erroll:*** Does this happen often?
Mr Fishenden: Not often, as far as I can recall, no. It is an occasional occurrence because a lot of the identified vulnerabilities are theoretical ones, if you like, at the time they are notified to us, so people prove there is a vulnerability in the lab environment and there is a usually a time window before someone then exploits that vulnerability in a real way.

Q294 ***Earl of Erroll:*** Is there not then a problem that they have got time to reverse engineer the patch to find out what those who did not know what the

vulnerability was, work the vulnerability and get something out there to attack the system before your patch comes out?
Mr Fishenden: Yes, it is a challenge for anyone in the industry. We have all tried methods of obfuscating patches, trying to hide some of what they are really doing by changing other things on the system that actually have no discernible effect upon it and so they cannot work out exactly what the patch did. Of course, whatever you do people can take a snapshot of the machine before you apply a patch and take a snapshot after and then people can start using that type of information to try and work out where the vulnerability might be, so yes, it is a very real problem.

Q295 ***Earl of Erroll:*** This has not been a great problem in the field, this reverse engineering, and then other viruses can gain access?
Mr Fishenden: Not to date. Where it does become an issue is obviously where you have a situation where somebody may not be automatically applying the patches, so although we have issued a patch maybe someone has reverse engineered it, released it and exploited it into the wild. It is the users that have left their machines unpatched that then become vulnerable to that line of attack.

Q296 ***Lord Sutherland of Houndwood:*** My apologies, my Lord Chairman, for being late but I want to ask a question that probably fits in here as well as anywhere. It is a naı£ve question and you will doubtless tell me if it is too naı£ve to answer, but tell me politely. How far are the standards of security that operate within your own organisation and the machines you use the standards that your customers can expect you to roll down to them, be they large business operators or home customers? Is there a big gap and is the gap what we can anticipate having, or are there serial reasons for having a gap of this sort?
Mr Fishenden: Essentially we use exactly the same tools our customers use. The one difference is that we have a thing called dog-fooding inside Microsoft where as part of our preparations to release a new operating system or new bits of software we install it, if you like, before it is necessarily ready. Probably a year ago I started running early builds of Microsoft Vista. Part of the purpose of that is that in a large scale environment, and we have 50,000/60,000-plus machines inside Microsoft, we are a very useful large-scale test bed for, as we call it, dog-fooding, which is putting ourselves through the potential pain and occasional delight of early adoption of software while it is still in development so that we can make sure that by the time it ships we have ironed out as many of the possible problems that could be anticipated with that platform as possible, so, although I say we are using exactly the same tools that people do outside Microsoft, in reality you would often find that a lot of us are on the next build of software that will be coming downstream later.
Lord Sutherland of Houndwood: Thank you. That is helpful; that is what I wanted to know.

Q297 ***Chairman:*** Peter Gutmann has recently suggested that you have seriously compromised the security and stability of Vista in order to provide content protection for premium content. How do you react to that?
Mr Fishenden: I am familiar with Peter Gutmann's article and it will not surprise you to hear that I take a slightly divergent view from Peter. The issue he was getting at is related to one of content protection and with Windows Vista, as with our existing PC platform, a lot of people are using it to watch DVDs, for example. The content providers, which are Hollywood and the movie industry, have set minimum standards that any platform that is going to run the next generation of high definition content that is coming must adhere to or it will not be able to run on it. That is as true of Windows Vista and our operating systems as it is of an iPod device or a dedicated DVD player that you might buy to use in the home. Anybody who does not adhere to the content provider's rules, their software is not going to work. That is the reason we have had to put those features into our platform. On the specific point of whether it compromises security at all, we do not accept Peter's points at all. He uses an example, I think, of medical images and saying that it would degrade the content and that is not true. Unless people are using and specifically invoking these content protection mechanisms for things like Hollywood movies the rules that apply to that content protection do not even come into play. If people are opening medical images and content to look at them, then it is not an issue. They open and are completely untamperable with. There is no loss of fidelity. There are no risks in using them. My summary is that we see these things as completely independent of each other. One is to do content protection, which we have supported on our platform for some time now. In existing DVDs there are companies like Macrovision which ensure that people cannot easily rip DVDs and we have put things into our platform to ensure that we meet the content provider's stipulation; otherwise people would buy a PC and then would not be able to watch a DVD and increasingly would not be able to watch HD-DVDs. We do not accept the point that we have compromised security in any way. In fact, if anything there is a hope that the very high quality device drivers being required for some of the high definition content coming out may result in a higher level of quality assurance around third party providers.

Q298 ***Chairman:*** Have you published a response to his comments?
Mr Fishenden: I believe my colleagues in Redmond are publishing one either as we speak, or certainly this week there should be something up on the web as our form of response, going through point by point the issues that he raised.

Q299 ***Chairman:*** Perhaps you could make sure we get that response if we do not find it for ourselves.
Mr Fishenden: Yes, sure.[1]

Q300 ***Earl of Erroll:*** One of the issues he has is that in many cases if you start playing high definition videos or DVDs, et cetera, the quality will be degraded if it is going via Vista because it has to run with certain combinations of broadband. If so, that will discredit Vista and its uptake would not be so great. Do you see that that could possibly happen?
Mr Fishenden: Yes, and again, if it is a high definition DVD the tools in Vista are designed to deliver you the high definition experience. If you are plugging it into a high definition, 10 ATI PC with an HDMI slot that also supports high definition content protection, then you are going to see a completely seamless high definition experience in the same way that you would if you went and bought a dedicated consumer electronic device.

Q301 ***Earl of Erroll:*** I think we need to see a technical rebuttal.
Mr Fishenden: Sure, okay.

Q302 ***Earl of Erroll:*** You refer to the industry-wide InfoCard initiative for exchanging identity credentials over the Internet, which might mean that some of the current rather simplistic password and user name systems change. Do you want to elaborate on that slightly?
Mr Fishenden: What we call Windows CardSpace, which is something that is already in Windows Vista and we are making available to Windows XP users, is our implementation of what we call an identity selector. There are many third parties working on this alongside us, and it is very encouraging, having worked in the IT industry for 20-plus years, I guess, to see such a collective groundswell of focus on tackling what is a very major problem on the Internet, which is that it is pretty well designed without the identity layer. It is very hard for us to prove who we are when we are on-line and we go and visit lots of third party sites and we are not really sure whether that really is our bank that we are about to provide our details to. What CardSpace does by analogy is bring the type of experience we are used to in the real world when you go into your wallet and you see all sorts of different cards, maybe a Visa card, a Mastercard, House of Lords access card, whatever it might be, and you know which one to use in a particular context. You know if you try and enter the House of Lords your Visa card is not necessarily the best way of getting past the doorkeeper. That may sound a simple analogy but in the on-line world it has never been that easy to use identities. What we are looking at doing is providing that highly visualised environment, that when you go to certain e-commerce sites this is the card you can use securely with e-commerce, you can move away from the user ID and password problem and all that goes with it, such as phishing and pharming and the like, but when you get to a different context, and that could even be within the same e-commerce sites; maybe you have established that you are the same person that came to On-lineBooks.com or whatever it is last time, you go to pay and at that point you might want to use a different card, which could be your Visa or Mastercard or American Express card, and again it can be a simple matter of identifying and clicking on that card within the identity selector. I guess we are trying to tackle several things at once. One is the user experience, so we are trying to get a very consistent way of using identity on the Internet which is much more intuitive for users. One of my colleagues, Kim Cameron, who has been one of the driving forces behind this, has used the phrase that we have almost been taught to be phished and pharmed on the Internet. It is true in a sense that because there is no consistency in the way we provide log-on details to different websites and try to authenticate whether we are genuine. It is very hard to pick up on the cues that might alert us to the fact that actually this is a spoof site, not a real one, so a lot of the attention has been behind trying to get consistency across the industry in how we use these identity selectors. You know how they work and you know when you go to the sites how they work, and if something looks unusual then there is probably something wrong because it is not working the way it should. I do not know what the analogy might be in the real world but I guess one might be restaurants that take your credit card and disappear for 10 minutes somewhere at the back and you are never quite sure what they may or may not be doing with it. The other part is securing the identity environment, making sure that you have a much better level of assurance that the information you are sending between the PC or whatever you are working on and the site is encrypted and protected, so, if you take the worst case scenario, somebody who has got spyware sitting on their PC, how we protect the environment so that people cannot see what cards are sitting in your identity selector, and if they are trying to fool you by showing you a different wallet that would be as alien to you as opening your wallet in

[1] http://windowsvistablog.com/blogs/windowsvista/archive/2007/01/20/windows-vista-content-protection-twenty-questions-and-answers.aspx

your pocket and seeing somebody else's bank cards and their different types of identity documents. I think it is a very encouraging piece of work. It has got to make contact with the real world yet, although this means cross-industry work going on. We are now at the chicken-and-egg situation that we have got the existing Internet as it is today with user ID and passwords, we have got CardSpace and identity selectors coming along, including some open source Java-based identity selectors, and we are now at that situation where we are going to need to find a balance of consumers and citizens seeing a benefit in using these new tools, but equally there has to be a producer push of banks, e-commerce sites and other people saying, "Here is an alternative way of you authenticating to our website", because unless we get enough of that happening at the same time people are going to find this facility available to them and no sites to support it, or vice versa, the sites start providing it and users are not aware that they can take advantage of it.

Q303 ***Earl of Erroll:*** CardSpace is, of course, the Microsoft implementation of the InfoCard. Given your dominant position, are you finding that you are getting cross-industry co-operation on this or is it seen as a Microsoft initiative? Are there other people producing incompatible InfoCards or are you trying to steal a march by making extra facilities available in CardSpace?
Mr Fishenden: We certainly do not want it to be seen as a Microsoft-only initiative because it will fail. Identity is a problem that everyone needs to crack on the Internet and we have deliberately been working for, I guess, two-plus years now with people you would not naturally expect us necessarily to be talking to, so people like Firefox, Apple and others, talking about what we are doing, being very open about it. All of the specifications on which we have built Windows CardSpace are open and in the public domain under the open specification promise, that anyone can use them, there are no royalties, there is no catch, if you like, to anyone taking this and building their own identity selector. On the point of view whether there are extra features in Windows CardSpace to other identity selectors, we are obviously doing our best to make our identity selector looks to be the best possible experience and most secure experience on our platform, but that certainly does not prevent anyone else from taking the specification. You can take it yourself, build your own identity selector, publish it openly if you want to or sell it commercially as a product and maybe have value added to it. There is certainly a good case to be made as CardSpace gains attraction, of looking at how it might also be used to secure data as it moves from one place to another, so we use it as a way of passing information very securely in an information-sharing environment and then using it as part of that overall architecture.

Q304 ***Earl of Erroll:*** So will we see anyone else's implementations on a competitive platform?
Mr Fishenden: Yes. There is already a Java open source implementation out there which has successfully been inter-operating with our system. Firefox have announced support, so their browser will support CardSpace's other identity selectors as well. All the signs are very encouraging. I guess it goes back to what I was saying about things not just being about the technology. I think we have got the technology in place. It is now trying to gain that impetus that really gets people moving from the current Internet which is lacking in sufficient identity tools to the one that is now in prospect.

Q305 ***Baroness Hilton of Eggardon:*** I imagine this is probably a question for Mr Lambert. You draw attention to the successes of self-regulation, in particular in relation to child protection. Would you like to see more regulation from EU or national governments and, if so, in what areas?
Mr Lambert: As you rightly say, we start from the principle that self-regulation seems to us a good system that works in many different areas, not just in these security areas. You would expect to hear that from industry people but it does actually seem to be true. There are one or two areas. One specific area the Government and perhaps the European authorities, the Commission and the Council, might want to look at is how you make it easier for ISPs and companies that have been damaged by spam or other types of cyber crime actually take direct action. It is quite difficult to be sure that third parties have a right of action, for example, against spammers. That situation here in the UK has been slightly clarified but there is no within-the-law clear set of damages for spamming. We pursue spammers all the time, for example. Last year we had a couple of very successful cases where we won damages, for example, Microsoft versus Naughty Cams. We won £45,000 worth of damages and most recently in December we had a case against a guy called Macdonald upheld in the High Court, where the judge said that we were, for the purposes of the British legislation, regarded as persons, Microsoft had been damaged. The way that he considered we had been damaged was that we are customers who have been damaged, we have had to spend a lot of money going after spammers, a lot of money on security technology to prevent spamming, and also we had suddenly to have a lot more servers that cost a lot more money because of the volume of spam. The issue there is that you can get the damages but you spend an awful lot of time going after those damages. One of the things that would be clearer

would be if a spammer is found guilty you can have a clear set of damages set down in the law. For example, you have got the US legislation which gives you this concept of statutory damages in this instance, so you have a per-spam fine which can be held against the spammer. That would, I think, act as a very considerable deterrent against spammers going into that market where they perceive on the whole that it is a crime that basically cannot be brought to account; it is very low cost to them and potentially a very lucrative business for them. So I think that is one small area where you could amend the legislation. I do think that is certainly worth considering. As I say, the courts seem to have clarified that to a certain extent to say that ISPs have a right of action, which is one area we were concerned to see. In Britain at least that does seem to have been clarified by the courts although it is not obvious from the legislation that that is the case.

Q306 ***Lord Harris of Haringey:*** You note in your evidence that cyber-crime and on-line fraud are not treated as priority indicators by the Home Office or UK police forces. You note that in the US there is a more unified approach to reporting such crime. Could you give us more detail about that American approach and what sort of indicators would you like to see introduced here?

Mr Fishenden: We believe it is necessary to have as easy a reporting mechanism as possible so that when people are victims of cyber-crime or attempted cyber-crime there is a streamlined reporting structure and ideally one body with responsibility for receiving those complaints and having appropriate resources to investigate and potentially initiate prosecutions where appropriate. As to the US (where my colleague Ed Gibson is probably the greatest authority on all things related to the US) certainly my understanding is that the United States does have a single point of reporting established by the FBI back in the late 1990s, the Internet Crime Complaints Centre, which takes some 10,000 plus complaints a year and has the authority and resources to actually look into those complaints. I note also recently in the UK the Metropolitan Police have made some public statements about the need for a consolidated UK-wide resource that could receive all reports of cyber-crime and have the resources. We are certainly very supportive of the police looking at ways of making it much easier to report. I have had that experience myself of being taken to phishing sites and the like and instantly knowing there is a problem but then of trying to find who I would flag up that information to. For someone who knows how to use the Internet quite well it took me an absurd amount of time to find some potential official reporting channels where I could flag up that sort of incident. Establishing that type of scheme, as happened in the States, would also enable us to get a much better grip on the scale of the problem in the UK. I suspect at the moment that might be somewhat fragmented because of the many different ways in which people might choose to report cyber-crime. For example, should you walk into a police station, is it going to be treated the same as any other crime? If I walked into a police station tomorrow to report on on-line phishing attack, would it be treated in the same way as an attempted pick-pocketing? Is that a model we want to move to or do we want to have cyber-crime handled at the centre?

Mr Lambert: If you look at the case in child protection on the Internet, the Child Exploitation and On-line Protection Centre—and I am aware you had evidence from the Chief Executive Jim Gamble last week—is a good model of where you have got one place obvious to people so that if you have got a problem which relates to child safety and you need to report abuse you can go to CEOP. That works extremely well and we work very closely with them, as do many other industry and NGO partners, and that is an obvious point of contact for everybody who has a problem or wishes to help with that problem. Likewise the Virtual Global Task Force of which CEOP and the British police are a part of this worldwide protection which I think you have already heard about. Again, in that area of security and safety you are moving to a situation where there is increasingly one obvious place to go if you have a problem, and that is very helpful in that case to young people and children who are being harmed. I think that is perhaps a good example of how you could improve these sorts of systems.

Q307 ***Lord Harris of Haringey:*** We also heard last week that electronic crimes, if we can call them that, are treated as traditional crimes just being carried out in a different way and pursued in that fashion. Obviously there are some virtues in seeing it as part of that continuum, so if there were a UK-wide simple, streamlined system as you describe how would you actually see that working in practice? Would it be separate from existing police forces and seen as just dealing with this or would it recognise that there is this gradation between more traditional approaches to fraud and the more modern phishing-type approaches?

Mr Fishenden: That is a challenging question. I was the victim of an attempted credit card fraud over the last weekend. Somebody had obviously skimmed my card or something, but where they chose to use it was on the Internet because they could go to many sites and attempt to order different goods. I think it does make a point which was alluded to a moment ago which is I think we do need to think as we move

forward about whether we make that distinction between cyber-crime and existing crime and establish parallel mechanisms or whether we recognise that it is crime enacted using the latest tools and technology, and they are going to evolve and change constantly over time and there are going to be unforeseen threats in the future around people misusing biometrics and the like as well as we move into the latest computing age, so I think you are right that we need to have a single point of reporting but then to make use of the existing police forces and resources as they exist today rather than try and build a type of parallel structure that somehow separates cyber-crime off from other crime because obviously there will quite be quite a close relationship between criminal activities happening in the digital environment, if you like, and the real world and they may all be aspects of a single criminal operation.

Q308 ***Chairman:*** Thank you, I am going to have to cut it off there because we have really run out of time, so thank you very much for your responses and thank you for giving us your time. If things occur to you that you think we need to know after this perhaps you would write to us?
Mr Fishenden: Yes indeed and we will pick up the earlier question as well, we will come back to you on that.
Chairman: Good, thank you very much for appearing before us.

Memorandum by Alan Cox

This submission attempts to summarise aspects of the open source community viewpoint on the questions asked by the inquiry, as was requested. It represents the personal viewpoint of the author based upon extensive experience and his position within the community. Although the author is employed in this field it does not represent the viewpoint of his employers and has not been reviewed by them.

Response to the Inquiry into Personal Internet Security

This response attempts to explain how the "open source" methods of software development used by projects such as Linux and Firefox relate to personal Internet security. Open source is a broad church and to cover anything but the generalities is worthy of a book not a response.

Defining the Problem

The Open Source community, generally speaking, is focused on two threats. The first is technical flaws in software which create an opportunity for attacks on systems. The second is attacks on the users themselves such as "phishing". Both threats are rapidly evolving in terms of attacks and countermeasures. As computer security increases, the attack target appears to be shifting as the user becomes the easier target.

The scale of the problem is difficult to measure and the open source community does not generate detailed end user data. It may also be misleading to think about it in a conventional crime recording model. Unlike a burglar who discovers a flaw in a common type of car lock, a software based attack can go from unknown to global within hours. This significantly changes the threat model and the required response. In particular, the open source community is sceptical of the longterm viability of virus scanners. These depend upon a reaction from a vendor and an update being issued before they can protect against a new virus. That may be too late.

The community does not track data on the number of users affected although data is tracked on the number of bug fixes made that may involve security. However it is very hard to relate bug fixes directly to actual incidents of user attack, as most flaws are fixed before they are exploited.

Open source users are probably atypical in terms of their understanding of the threat. There is a higher percentage of technical users in the open source community. Nevertheless there are some concerns within the open source security community that some of the less well informed attitudes of endusers may be problematic. In particular some users believe that open source software is totally secure and there will never be a risk of viruses or other problematic attacks.

Tackling the Problem

The number of flaws in open source software is lower than average. This has been measured by academics and commercial organisations using tools which look for flaws in software.[4, 5, 6] The public nature of the source code also allows extensive peer review of the code for quality. More popular programs generally get more review. The public nature of the code also makes it possible to search through all the code for all the programs in a system. This is important because a newly discovered flaw is often a mistake that will have been repeated in many other places. Having access to all the code allows screening on a large scale.

Developments in tools that identify flaws more rapidly, and languages that make it harder to write insecure code, are followed actively in both the open source community and the proprietary sphere. Extensions to computer hardware that are useful for security are also used; although many hardware features touted by vendors to be for security are actually mostly for marketing and not as useful as they would have the world believe.

Open source, particularly Linux, has also focused on making users secure by default. Red Hat Linux shipped with a built-in and automatically enabled firewall for years, something Microsoft has finally followed. This has led to new attacks being increasingly targeted against the web browser which must talk through the firewall, rather than against the system itself. Each step taken to improve security triggers a response of this nature.

Fixing software flaws is only one part of the process. For these fixes to be useful, endusers must be able to obtain them, verify they are correct and install them easily. Open source systems use management tools to automate this process, and digital signatures to verify that the code obtained is the correct code. But non-broadband users face a huge barrier. Fixes are not small, and the packaging methods are not currently optimal either. Thus we face the same problem that proprietary vendors face: users with limited connectivity are vulnerable to attack because they lack the ability to update their system.

Attacks directed at the user of a computer are much more problematic. Some defences are also hampered by US patent concerns which prevent the deployment of certain technologies which can help identify fake emails. In the UK there are also concerns about libel risks that make it hard, if not impossible, to keep the kind of databases needed to identify phishing attacks.

The open source community is following several strands of work in this area. Good user interface design can help to guide users to the correct choices. However there is a permanent conflict between ease of use and security. This conflict is difficult to resolve. Tools like SELinux implement security policies that extend further than traditional access rights. With such tools it becomes possible for a company to encode and enforce some company rules in software instead of depending upon education. For a variety of reasons (notably that the rules are in the company's interest, not the users') education rarely works well. For example it becomes easier to control who can run downloaded files or install software. This is important as it turns a security breach into a helpdesk call inquiring why the user cannot perform the undesirable act. It is a general opinion that the focus of attacks on confusing and misleading the user will continue to grow as the potential for attacks on software flaws decreases.

Governance

The international nature of the Internet requires international governance. Unfortunately the open source experience of regulation of the Internet and technology in general has been extremely poor. There is deep distrust of the establishment. The EU in particular is generally seen as the tool of big industry, lacking both transparency and control over lobbying.

Currently proposed and actual regulation affecting the industry includes the EUCD, rules on encryption export, and proposals to license computer security workers. These are likely to have strong negative effects on the open source community. Proposed regulation has already triggered responses that are not those desired by government: open source cryptography tool developers are completing software to render obsolete the government's proposed legislation on access to encryption keys.

The biggest barriers affecting security in the UK are probably:

— proposals in the EU for the adoption of software patents, making it impossible for people to implement some features even when they are critical to security; and

[4] B P Miller, D Koski, C P Lee, V Maganty, R Murthy, A Natarajan, and J Steidl, "Fuzz Revisited: A Reexamination of the Reliability of UNIX Utilities and Services", *Computer Sciences Technical Report #1268,* University of Wisconsin Madison, April 1995. http://www.cs.wisc.edu/~bart/fuzz/fuzz.html

[5] http://www.Internetnews.com/devnews/article.php/3448001

[6] http://www.prnewswire.com/cgibin/stories/pl?ACCT=104&STORY=/www/story/03062006/00043137 56&EDATE=

— the proposed updates to the Computer Misuse Act which make it unclear whether possessing a tool for breaking into a computer is an offence even when such ownership is for the purpose of security testing and software debugging and development. This will reduce security testing and discourage people from working on security (This is the area Lord Northesk has been attempting to correct).

It would be difficult to summarise the open source community view on improving governance of the Internet as it spreads such a wide political range.

Memorandum by Adam Laurie

Introduction

1. The author has been involved computing since the early 1980s, the Internet since it's inception, and Internet/Network Security in particular for over 15 years. His area of expertise extends from the Internet to mobile devices and communication protocols in general. He is a regular speaker and trainer at international security conferences, and is currently Technical Director of The Bunker Secure Hosting Ltd.,[7] of which he is also one of the founders.

2. Although this written evidence mainly concerns non-Internet related technologies, it is important to note that these technologies can be used as components of wider attacks which may include use of the Internet, or, indeed, the Internet may be used to provide access to data which could then be used to attack one of these technologies (as can be seen in the case of RFID enabled e-passports in section 3 below).

3. This written evidence is provided by the author as an individual.

4. In order to keep it short, as requested in the original call for evidence, this paper is far from exhaustive. Subjects covered here are intended to address the area of "Defining the problem", and will be in the fields of:

— Bluetooth.
— RFID.
— WiFi.

Bluetooth

5. Bluetooth is an RF based wire replacement technology operating in the 2.4GHz band.

6. The Bluetooth brand and IP is owned by a trade association called The Bluetooth SIG.[8]

7. It is commonly used for connection of Mobile Phone to Headset and PDA to PC/Laptop.

8. It is capable of carrying Data and/or Voice traffic.

9. Problems with Bluetooth were first publicised in November 2003 by the author,[9] concerning theft of data from mobile phones. This was dubbed "BlueSnarfing".[10]

10. BlueSnarfing is defined as "Taking an unauthorised copy of data via Bluetooth".

11. Certain models of Mobile Phone were found to be vulnerable to BlueSnarfing attacks, in which complete phone books, calendars and other information including the IMEI (the handset's unique identifier which can be used for phone cloning) could be retrieved without the knowledge or authorisation of the owner. This process typically took around 15 seconds.

12. Theft of data in this way could lead not only to further loss if information such as house or business alarm codes, or credit card PIN numbers etc were stored in the device, but also embarrassing or compromising breaches of confidentiality, as in the case of Paris Hilton's phone book, which was allegedly Bluesnarfed in February, 2005.[11]

13. In April 2004, similar controversy surrounded the revelations provided by Rebecca Loos selling confidential text messages between herself and the England footballer, David Beckham. In this case the owner of the messages herself chose to hand them over to a newspaper, but it is clear that the technology existed, had they but known it, for an enterprising 3rd party to obtain the same information (and more) without her consent.

[7] http://www.thebunker.net/
[8] https://www.bluetooth.org/
[9] http://www.thebunker.net/security/bluetooth.htm
[10] http://trifinite.org/trifinite_stuff_bluesnarf.html
[11] http://technology.guardian.co.uk/online/news/0,12597,1423271,00.html

14. Although performing a BlueSnarf attack is illegal, so gauging the true scale of the problem is impossible without breaking the law, it is possible, within the law, to estimate the number of vulnerable phones by a process of statistical estimation. By scanning in public areas for visible Bluetooth enabled devices, and profiling those devices to determine their vulnerability status, it is possible to obtain a rough idea of the scale of the problem. Tests performed in London, on the Underground system, during rush-hour in November 2003, revealed that in a fixed location (Victoria Station), approximately one potentially vulnerable phone passed by every 10 seconds.

— It is likely that this number is now far higher, as the number of Bluetooth enabled devices entering the market has been increasing steadily, although this is balanced by many of the security issues having been rectified by the manufacturers.

— Shortly after this test, an independent researcher in Austria, Martin Herfurt,[12] performed tests at a local trade show, and found approximately 1,200 potentially vulnerable devices over a four day period.[13]

15. Mr. Herfurt also went on to reveal further problems with Bluetooth devices, known as BlueBugging,[14] in which, amongst other things, SMS messages could be read, written and deleted from devices, as well as sent over the GSM network, again without the owners consent or knowledge. This leads to a number of issues:

— Victim liable for cost of messaging service.

— Interception and/or Loss of incoming messages.

— Impersonation of victim as messages appear to come from their number.

— Potential for attack on other services where SMS messaging is used for end-user authentication (such as Web Portals, Web Mail etc).

— Victim liable to be tracked via Internet GSM Tracking services. In this attack (known as BlueStalking), the mobile phone number is entered into a Web-based GSM tracking service, which will then authenticate via SMS text message. Once this message has been acknowledged, it is possible to determine the whereabouts of the device, displayed as a marker on a map, any time of day or night as long as the phone is switched on and visible to the GSM network.[15]

16. In addition, voice calls could be initiated, which leads to a set of further issues:

— Victim liable for cost of call.

— Revenue generation for 3rd party via calls initiated to Premium Rate services.

— Interception/Diversion of incoming calls.

— Impersonation of victim.

— Mobile Phone being used as a listening device by initiating a call to the attacker who can then monitor any conversation in the vicinity of the phone.

17. In the case where the phone provides built-in modem and/or networking facilities, it is possible to use the device to connect to the user's Internet Service Provider, or, even worse, to private back-end or corporate networks—the victim's device may then be used to launch untraceable attacks on 3rd party or internal corporate sites, or as a gateway for unsolicited email (SPAM).

18. Finally, using BlueBugging techniques it was possible to modify the storage areas on victim devices, including the phone book, which could lead to more problems:

— Man In The Middle attack: by modifying an entry to dial a voice bridge instead of the intended number, it would be possible to then create an outgoing call from the bridge to the originally stored number and connect the two calls together. To the victim pressing the speed-dial on their phone, this would not be apparent, but the voice bridge would then be in a position to monitor both sides of the conversation.

— Compromising entries added to Calendar or Phone Book.

19. All of the above problems have a potential bearing on mobile phone forensics, as the data found on the phone (or lodged with the service provider relating to the phone) can no longer be relied upon if the device is known to be vulnerable to these kind of attacks.

[12] http://trifinite.org/trifinite_group_martin.html
[13] http://trifinite.org/Downloads/BlueSnarf_CeBIT2004.pdf
[14] http://trifinite.org/trifinite_stuff_bluebug.html
[15] http://www.verilocation.co.uk/mobile_phone_tracking.aspx

20. Within 12 months of these revelations, The Bluetooth SIG initiated a security testing and awareness program within their development community by facilitating prototype and production model device testing at their tri-annual industry interoperability events known as "UnplugFests".[16] These are held over a one week period and most of the major mobile phone and PDA manufacturers participate, as did the author.

21. As of October 2006, Security Testing at the UnplugFests has been discontinued, the author is under NDA regarding the details of work undertaken at the UnplugFests.

RFID

22. RFID is an acronym for "Radio Frequency IDentification".[17] It is commonly used in building access control, retail security and animal identification.

23. Trials under way for credit card replacement/enhancement, and machine readable travel documents such as e-passports[18] are already in common use.

24. Typical form factors are plastic card, key fob or injectable glass pellet.

25. Many forms of RFID rely on a unique serial number programmed into the device at time of manufacture for their security. Manufacturers make much of the guarantee of "uniqueness" of the serial number, and therefore the security of the device or the system secured by it.

26. Potential problems are cloning, skimming, relaying and profiling/tracking:

- Cloning is the process of producing a functional copy of the device. Experiments have shown that it is possible to imitate more or less any form of RFID tag with specialist equipment, which, although custom built, is not particularly bulky or costly, so could be effectively deployed.[19]
- Several demonstrations of this technique have been performed at security conferences worldwide,[20] but the full ramifications are often lost in the debate as to whether a device that does not follow the original form factor is a true clone or not.[21]
- The author has found it is relatively simple to produce a "true" clone of many supposedly "impossible to copy" devices, such as the EM4102,[22] which not only contains the same serial number as the original, but also follows the same form factor. The full details have not yet been released into the public domain, but the Author can provide demonstrations on request.

27. Additional security measures such as cryptography may be applied to protect data stored in the RFID device. An example of this would be the e-passport:

- A cryptographically protected device requires a key to be known to the reader in order to authenticate and to decrypt the data stored on the device.
- In the case of a device such as an e-passport, this key must be easily available to authorised users, such as border guards, immigration officers etc, whilst still being secure from unauthorised users. This is achieved by deriving the key from data printed on the identity page of the passport itself, which is made visually available to authorised users, but, in theory, remains unavailable to an attacker.

28. The problem with this scheme is that the data required to derive the key may be available through other channels. In the case of the e-passport, the key is derived from the passport holder's Date of Birth, the Passport Number and the Expiry Date of the passport (there is a further optional field included in the calculation, but in all cases so far seen by the author, this field has been blank).[23] All of this information is included in the data required to be submitted to the US Homeland Security Agency under the Advanced Passenger Data agreement:[24]

- The author has shown that poorly configured airline websites can leak this data,[25] and, even if that were not the case, the number of individuals with access to the data (web designers, maintainers, internet service providers, software engineers etc) is sufficient to give cause for concern.

[16] https://programs.bluetooth.org/upf/
[17] http://en.wikipedia.org/wiki/RFID
[18] http://www.passport.gov.uk/general_biometrics.asp
[19] http://cq.cx/proxmark3.pl
[20] http://cq.cx/verichip.pl
[21] http://www.aimglobal.org/members/news/templates/rfidinsights.asp?articleid=1535&zoneid=24
[22] http://www.emmicroelectronic.com/Products.asp?IdProduct=5
[23] http://www.icao.int/mrtd/download/documents/TR-PKI%20mrtds%20ICC%20read-only%20access%20v1_1.pdf
[24] http://www.britishairways.com/travel/ba6.jsp/imminfo/public/en—gb#us
[25] http://www.guardian.co.uk/idcards/story/0,,1766266,00.html

— This gives rise to the possibility of skimming the passport, as well as cloning it.

— Cloning of e-passports has already been demonstrated by Lukas Grunwald, a German security researcher.[26]

— Reading of the data contained within e-passports can be demonstrated by the author, using low cost, off-the-shelf RFID equipment, a laptop, and his own software.[27]

WiFi

29. WiFi is a generic term for Wireless Local Area Networking.[28]

30. WiFi networks are used to provide local connectivity to both home and office users, and would typically be configured to provide Internet access for multiple computers around the building without the need for expensive or disruptive cabling, by using RF operating in the 2.4GHz and 5GHz bands.

31. There are typically three modes of security for WiFi:

— Open. In this mode there is no encryption of over-the-air traffic and all data is visible to anyone within range of the WiFi base station.

— WEP—"Wired Equivalent Privacy".[29] This protocol provides encryption for all WiFi traffic, and purports to protect the user from unauthorised access to their network, or "sniffing" of broadcast traffic. Unfortunately, the encryption used in the WEP protocol was shown to be fundamentally flawed by researchers at Berkely in 2001.[30]

  Despite this, five years on, WEP continues to be shipped as standard on most WiFi equipment, and is probably the most common form of protection in use today.

— WPA—"WiFi Protected Access".[31] This protocol and it's variants are intended to replace WEP and provide a much higher degree of protection. Most modern equipment is capable of providing this standard.

32. WarDriving[32] is the process of searching for WiFi networks whilst driving, and plotting them on a map. An Internet visible map of WarDriving data can be found at "Wigle", the "Wireless Geographic Logging Engine",[33] which, at the time of writing, holds over 8 million individual WiFi location records worldwide. From this map it is clear that very large numbers of unprotected or WEP protected WiFi networks have been deployed in the UK, and are therefore vulnerable to attack.

33. Attacks on WiFi networks potentially cover the entire range of possible attacks on network connected computers, and so are beyond the scope of this paper, but suffice it to say that as well as loss of data through "sniffing" of over the air traffic, the potential for direct installation of key loggers, trojans, viruses and other malicious code exists, as does the possibility of using the compromised network as a launchpad for attacks on other Internet connected systems.

Conclusions/General Observations

34. It is often the unexpected interaction between systems, or the addition of new technologies to otherwise reasonably mature devices that leads to security issues—For example, adding Bluetooth to mobile phones led to compromises of services that had previously been secure, such as OBEX File Transfer (Bluesnarfing) and RFCOMM (Bluebugging).

35. Manufacturers have a tendency to put "user-friendliness" before security on their list of priorities.

36. Security may not be part of the initial design process on a new product, and tends to be added or given proper consideration only after problems occur.

37. When security is considered in the initial design, it may be looked at too much in isolation of other factors surrounding the deployment of the technology—for example, e-passports have strong cryptography protecting their contents, but this is weakened by the availability of the data required to generate the cryptographic keys, and thereby access the "secure" passport.

[26] http://www.wired.com/news/technology/0,71521-0.html?tw=rss.index
[27] http://rfidiot.org
[28] http://en.wikipedia.org/wiki/Wifi
[29] http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy
[30] http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
[31] http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access
[32] http://en.wikipedia.org/wiki/WarDriving
[33] http://www.wigle.net

38. It is very unusual for a product to be "recalled" due to security issues. In devices such as mobile phones, problems may be fixed for future releases, but thousands of vulnerable devices are left in the field, their owners largely unaware that they are effected by the problem.

21 October 2006

Examination of Witnesses

Witnesses: Mr Alan Cox and Mr Adam Laurie, examined.

Q309 ***Chairman:*** Welcome Mr Cox and Mr Laurie. Thank you very much for coming today and addressing our questions. Would you like to introduce yourselves first please.
Mr Cox: My name is Alan Cox and I am here to represent the open source community in general. That is a bit different perhaps to representing a company but it is a broad church and I am trying to summarise its views rather than being a dictator of those views.
Mr Laurie: My name is Adam Laurie and I am a director of a secure hosting data centre called The Bunker and I am also an independent security researcher and a participant in security conferences around the world.

Q310 ***Chairman:*** Thank you. Would either of you like to make an opening statement or should we go into the questions?
Mr Laurie: I would just like to say when I look at Internet security I tend to look at it not just from the point of view of securing the Internet but also how the Internet can be used as an attack vector against other areas of life. I take a very broad view. We had some examples of credit card details being stolen by skimming and then used on the Internet and the same can be vice versa, so I may drift off into other areas of communication and personal security.

Q311 ***Chairman:*** Right, good, thank you for that. Let me open with the first question and that is: who should be responsible for keeping end user machines secure?
Mr Cox: I would take a similar line to the Microsoft people. Certainly there is at least a moral duty on people providing software to do their best to produce software which is secure and as best as possible that is fit for purpose. The problem we have throughout all computer sciences is that we genuinely do not know how to build a perfectly secure, useable operating system. It is a research problem which one day will get solved and somebody will get very rich out of it, but the current state of affairs is that we cannot do that. Much like the way you have to maintain a car, we rely, to an extent, on end users being able to apply updates, in the same way your tyres wear out and you need new tyres on a car. That is not a manufacturer responsibility; it is an operator responsibility so you have to spread it across the two.
Mr Laurie: I broadly agree with that. I think it is the duty of manufacturers to make it easy for you to make things secure. I am very pleased to see that Microsoft are now shipping secure by default settings so the file latch is switched on, which has been something that the open source world has also worked their way up to. They did not start doing things that way round but we found it is better to make the machine secure by default. However, you do have to provide the tools, advice, timely updates and advisories when there is a problem in order for the user to make their own choice as to whether or not they want to apply a particular patch or how secure they want to be. As has already been said, there is always a tradeoff between usability and security. What I think is very important is that we do not try and make manufacturers or vendors responsible because there are just too many factors for them to be aware of in an installed user base. You ship in an operating system and users will then stick third party products on top of that which may affect the security of the system. There is no way that a vendor can be aware of that and you will tend to end up in a situation where there is finger-pointing going on, the operating system vendor will say it is the third party software that is at fault and the third party software vendor will say it is the operating system that is at fault, and there will be grey areas where unexpected interactions cause insecurity when both products on their own are perfectly secure. It would not be fair to put that burden on the vendor. In the open source world as well there is a particular issue with liability. How can you make an open source vendor liable for a product that he has given away for free? There is no contract, there has been no consideration for delivering the software, so there is no way to enforce liability on an open source product.

Q312 ***Chairman:*** At the same time a larger community works on it so do you think we should encourage people to use open source software?
Mr Laurie: Absolutely. I believe that we are going to talk about the relative security of open source and closed source but I do not think the issue of liability should actually prevent you from using the software. With open source software you can see for yourself whether it is secure or not and do something about it if it is not. With the closed source software there is more of a promise by the vendor that a piece of software does what it is claiming it does. With open source it tends to be, "Well, this is the product and

you can see for yourself what it does, but we make no promises. If you want to improve it then join the project and help to improve the software."

Q313 ***Chairman:*** So you would say ultimately that manufacturers supplying the software should accept legal liability for losses caused as a result of security holes?
Mr Laurie: No, I am saying they should not be held liable.
Mr Cox: I do not think they can be. The response of any rational software vendor if they were told they were liable because of this business about adding software in combination would create a combatorial explosion. So for example, you buy a PC, you add a word processor, you add a media player, and you add a couple of games. All these can interact in strange and wondrous ways and as you add more software the combination increases. The rational thing for a software vendor to do faced with liability would be to forbid the installation of any third party software on the system. That would be the only behaviour that would be sensible. I do not know, however, whether there is an argument in the longer term that as technology improves and as we get better at writing secure software that the law does need to hold software companies to higher standards, at least in terms of negligence and areas where there is room for interaction. When talking about the open source offer, although the open source offer is generally given away by the people who develop it, there are companies around that software and most people who are end users or business users probably buy some kind of package of CD software and support rather than necessarily just getting the software for free. The question relates to how liability moves with the services and with the other parts of the product. At the moment there is a strange behaviour where if the CD is faulty you clearly have recourse. If the software on the CD is faulty the situation is clear, but that is the same throughout all sorts of services and non-physical goods in the European Union. It is not just a software problem, it is a very big problem. There are certain security people within the open source community—although it is not by any means a universally held view—who hold the view that one of the reasons that we have problems with computer security, as we have problems with many other things, is where those things have no recourse, no liability attached to them. There is nothing forcing standards to be reached or forcing quality to happen, and providing some kind of mechanism to persuade vendors to do the job right.

Q314 ***Chairman:*** Do you have feelings about Wi-Fi and the fact that many people install it without any real security on it, in terms of logging into a local network if not being able to get into the computers themselves? Do you think Wi-Fi should be compulsorily pre-installed with security?
Mr Cox: I think Wi-Fi is a perfect example of why you should have security by default. Wi-Fi is in the state today as most vendors of Windows products were seven or eight years ago in that the default is that security is not turned on in most cases. Some of them now turn security on by default and we should be glad of that because the default for any product which has the ability to cause harm should be that the harm-causing features are disabled, so you have to learn what you are doing and understand what you are doing before you put yourself at risk.
Mr Laurie: It should definitely not be compulsory because in some cases you want your Wi-Fi access point to be wide open. There are many people who are part of a community of Wi-Fi sharing so they not running hot-spots in a commercial environment but they are running the equivalent of a Wi-Fi hot-spot at home where they invite neighbours or anyone in the area to use their Wi-Fi and in return they expect other Wi-Fi points to be available on their travels wherever they want to use it.

Q315 ***Chairman:*** You don't think Starbucks would like to give an access code to everybody they sell a cup of coffee to?
Mr Laurie: Starbucks might want to worry about people sitting in their cafes sending spam and so on so there will always be commercial considerations as to why you might want to protect your network. I think the question of liability again here is potentially there should be some issue of liability for companies shipping products that are known not to be secure and selling them as secure products. There are some specific issues with Wi-Fi where protocols like the WEP protocol was broken a long time ago and yet they carried on shipping it and telling the public that that was a secure protocol when it demonstrably was not.

Q316 ***Lord Howie of Troon:*** I think Mr Laurie has come fairly close to answering my question already which is; is open source software more secure than closed source software and if it is can you tell me why?
Mr Laurie: That is the $64 million question and that debate will rage forever and you will get arguments on both sides. From the open source perspective, we believe it is more secure because it is subject to more scrutiny and peer review and so on. You can look at the code yourself and see if it is secure or not. You can cross-check against known problems, so for example when an issue arises in one product you can look at how that issue actually came to be and whether other products are subject to the same problem. If it is a low-level library that has been used in the compilation of that product that is at fault, you could look at other open source products which use the

same libraries and see if they are also affected. That is a process that routinely goes on. If there is a publication of a security issue in product A anyone who knows the source code will immediately go and check their own products to see if they are also affected. So you get a very rapid dissemination of security fixes in the open source world. As an example of the security of an open source product, there is a web server many people will not have heard of called Apache. Quite often when I am speaking at a high-level conference I actually ask the question of the room, "Who here has heard of Apache?" and maybe 10% of the people in the room will know. I will then ask, "Who has heard of Microsoft?"—big laugh, of course everyone knows Microsoft, and then it surprises them to learn that Apache SSL, which is the secure web server version of it, has 70% of the world market in secure servers. In its ten-year history there have only been three security alerts and two of those were because of external libraries that were being used, so there has only ever in its 10 year history been one issue specific to Apache SSL itself. On the other side of the coin, the closed source world relies on what we call "security by obscurity", so you are secure because the problem is not visible. That does not mean the problems are not there; they are just harder to find. So talking about the bad guys, if there is money to be made out of a security issue the bad guys are going to find it. They will poke around and they will dig around. Securing software by simply hiding the source code is like putting paper on the wall and saying you cannot find the windows. If you poke enough eventually you will pop through a window. The other issue with closed source is there are often commercial factors involved in whether or not they release security information or they fix a problem. If they believe that they are the only people who know that there is this particular security problem they may choose to do some damage limitation not to admit to the problem because it will damage their image too much. They do a risk versus reward calculation and decide the three people who are likely to find this problem or report this problem are not going to come forward so they are not going to bother fixing it unless it turns into a live issue. The open source world has no such limitations because we do not care, we have no liability, so as soon as an issue comes to light we will publish, and usually that will be within hours of the problem coming to light. Again the closed source world tends to take longer to react. They have a lot of infrastructure that needs to catch up, notifying their paying customers, printing manuals possibly, distribution and so on, so there are a lot of factors that affect the distribution of the fix that are harder for the closed source world to deal with than the open source world.

Q317 ***Lord Howie of Troon:*** When you mentioned covering over windows earlier on, you were referring to, I presume, the security holes?

Mr Laurie: Yes so a brick wall with windows in it and a sheet of paper over it.

Q318 ***Lord Howie of Troon:*** If the windows which are the security holes are not covered over are they not therefore by definition easier to find?
Mr Laurie: Absolutely, easier to find and easier to fix. The open source world relies on scrutiny so obviously you believe that your open source product is secure, you have released it into the world and people are using it. If an unexpected issue comes along it is much easier to see what is going on. You have many eyes looking at the problem and very often an open source problem will be fixed literally within minutes or hours of the problem coming to light, and that fix will then be available to the public because of the distribution mechanisms that open source employs. It will not have to wait a month or until the next patch Tuesday to get released to the public.

Q319 ***Lord Howie of Troon:*** That makes you wonder. The security holes are found by what you call the bad guys but are they necessarily identified by the good guys at the same time?
Mr Laurie: There is a lot of research being done not just by the bad guys but also by the good guys. The ones the bad guys find obviously they will try and keep to themselves but they also need to exploit them and as soon as they start exploiting them they start leaving a trail that this problem exists and then the good guys can come along and try and find how that problem came to be. There is also a huge community commonly referred to as "hackers" who are not hacking for bad, they are hacking for good. We refer to the bad hackers as "crackers" and everyone else as "hackers". They do it as an intellectual challenge. This is another debate which will rage and rage, what is the definition of a hacker, but there are hackers who do it for the good of the community and trying to find security problems before the bad guys do.

Q320 ***Lord Mitchell:*** Going on from that, I wondered what your views were of Microsoft's automated security patching system? Does it not seem that it is somewhat ahead of what other open source systems can provide?
Mr Cox: I had a look at this one. The first automatic update software in the open source world was about 1998. It is actually one of the things where open source vendors compete against each other. One of their key differentiating factors is the way they provide these kind of automated update services. I would take the view that except for dial-up users where there is a real problem with all products because the size of software their updates require does not fit very well down the modem. It is a solved problem now in the free and propriety world. I think we are sorted on that one, both in the open source

world and the Microsoft world. The automated updates are there, they are working. There are questions about the timeliness of delivery of patches and that sort of thing, but not about having an automated update system.
Mr Laurie: I would agree with that. I think it is a very good thing that Microsoft now provide automated updates and the only limitation really is the time limitation. However, what they provide patches and updates for is the Microsoft operating system itself. In the open source world you will find that the patches also include most of the third party software that you have installed so the open source world has a much broader coverage on automatic updates than Microsoft.

Q321 ***Lord Mitchell:*** What is your opinion of the Vista operating system?
Mr Laurie: I think it is a very good thing if it works. I have not been playing with it. It is not publicly released yet. I personally do not use Windows; I use a Linux derivative. I have not used Windows for as long as it has been around.

Q322 ***Lord Mitchell:*** Do you think it goes some way to satisfying some of the criticisms of earlier versions of Windows?
Mr Laurie: I think they are certainly trying. Microsoft to their credit really do listen to the open source community, the full disclosure community, and the security community. They participate a lot in security conferences and so on and they listen. I think they genuinely try to create a secure environment and I applaud them for that.

Q323 ***Chairman:*** Mr Cox, do you think Vista is the most secure system that has ever been produced?
Mr Cox: In the general case it is certainly not the most secure system, but the really secure systems have always been produced for things like military use where usability is not a factor. Whether it is the most secure operating system for the desktop we will really have to wait six or 12 months to see to what the figures are for malwear problems. I agree with Adam on this, Microsoft have clearly made a good effort here. There are a lot of things where open source versus Microsoft goes on in the marketplace but security is very much the vendors versus the fraudsters, we are all on the same side.

Q324 ***Earl of Erroll:*** Mr Cox, in your written evidence you both suggested a need for international governance of the Internet and you also expressed distrust of governmental regulation hitherto. Could you describe in more detail how you would like to see the Internet regulated.
Mr Cox: What has caused a lot of annoyance and problems in the open source world has been regulation which is controlling tools, things like control of encryption, control of possession of software which is useful both for testing and exploiting machines which, unfortunately, is the same software. People often describe it as "thought" crime, offences which have no victim which should not be a crime. At the same time, if you are dealing with a real incident where damage is being done and fraud is being committed, it is very, very hard to do anything about it. Firstly, fraud is almost always international so you trace it back and you find you are being attacked by a Polish machine controlled by somebody in Nigeria who may or may not be working for an American. Needless to say the system is not well adapted to this in computing or outside of computing. The second point is that the UK police, at least if you walk up to the desk sergeant at a typical police station—and I have a friend who has real experience of this—he does not understand the problems (and why should he) and there is then nowhere else to go. So a local music shop for example suffered some real problems with spammers misusing their name, attempting to really do them damage and to destroy their reputation. When they approached Swansea police station the Swansea police were perfectly willing to help, they really wanted to do the right thing but did not know enough to do anything about it, and so we need something which deals with electronic crime and computers, either an understanding in police stations or we need a central contact point. Also with this you need to act fast. One of the things about phishing attacks is an email gets sent to one million people designed to trick them to use some site. If you shut that site down in an hour for most of those people by the time they get the email the site is shut down. If you shut that site down in 24 hours, you have probably made no difference so a very, very fast response is sometimes needed to these things.

Q325 ***Earl of Erroll:*** Right, so a lot of it is not necessarily so much Internet governance as cross-border co-operation and also internal police responses, which are really your concerns?
Mr Cox: I suppose in a sense we need to police the Internet in the same way as we police streets. Whether that is governance or policing I am not quite sure.

Q326 ***Earl of Erroll:*** The other thing that came out was that the open source community in some ways regarded the EU as the tool of big industry. Why is this? Is it the dispute between the EU and the Commission and Microsoft where Microsoft appears to be in breach of anti-trust laws and taking defensive positions, that sort of thing?

Mr Cox: No, it is particularly to do with software patents where there is a very distinct lack in the European Parliament of control of lobbying, declaration of interests, this kind of thing. We have found it very, very hard to work at getting our point across in places like the European Parliament whereas the big companies are able to spend huge amounts of money and that has been used in various ways particularly by the media companies, so we have had various instances of things we used to be able to do which we are not allowed to do, but they fall outside of Internet security.

Q327 ***Earl of Erroll:*** Are some of those software patents inhibiting your efforts to increase security?
Mr Cox: They are. There are both legal and patent ones. The legal one in the UK is partly the Computer Misuse Act, particularly the recent update which is going to cause problems, and also the libel law. The computer misuse side of it will cause a problem because it is now an offence variously to possess tools or give people tools which can be used to break into computers, which are unfortunately the same tools that you need to identify the security holes and test a security hole has been fixed and so on. The Crown Prosecution Service was supposed to produce guidelines on this issue but we do not know what those guidelines are yet. It is not clear what will happen about private prosecutions. There is a worry that disreputable companies might try to use that law to shut down legitimate reports of security holes. If you are trying to do things like anti-phishing what you want to do is create a list of phishing sites, so at nine o'clock in the morning I get this email in "there's a fake Lloyds Bank site" and you put it on the list of fake sites. People check that list and it puts up a thing when they go to it which says "this may be a phishing site". In most areas of the world if you do that and you get it wrong you might be liable to pay a few thousand dollars to somebody who lost business. In the UK all the lawyers will say is just do not do it. The patent one covers patent claims on various things, particularly things like secure mail checking. There has been some progress on that since the written evidence. Microsoft owned at least one of those patents and they used to have a multi-page dreamer whereby you could use it but it was completely unworkable for most organisations. The recent draft they had approving this is one page long and appears to solve the problems, so there is progress being made there as well.

Q328 ***Earl of Erroll:*** You seem to be against the concept of licensing security professionals. Would it not be safer to have some method of trust in the people who are likely to be working on our computers?
Mr Cox: From the open source world point of view most security work is not done by security professionals, by trade; it is done by students, done by volunteers and some of it is done by professionals. If you were to try and regulate and control who is a security professional, what you will actually do is forbid a large number of people currently fighting the bad guys from taking part. It is almost like saying you are not allowed to help fight crime unless you are a policeman.

Q329 ***Lord Harris of Haringey:*** Looking at the whole range of communicating computer-based devices, what do you see as being the main vulnerabilities affecting private, individual users?
Mr Laurie: Currently the obvious attacks that are going on are mostly theft of credit card details, attacks against e-commerce, identity theft, phishing, scanning and then using those details to attack on-line banking or even taking it off-line and buying goods through traditional methods using the details obtained. I think the problem of spam and viruses and malwear is ever expanding.

Q330 ***Lord Harris of Haringey:*** I am just wondering if you are answering a different question. What I am interested in is most of us in this group are probably carrying mobile devices of some sort which have access to the Internet, do e-mail and things like that, and there is a whole new generation of iPods coming along we have heard much about in the last few days and so on. I would be interested in—and I think you alluded to it in your opening statement—where that leaves the individual user in terms of vulnerabilities.
Mr Laurie: In the future mobile devices are becoming more and more tightly integrated into our lives and there is a convergence of media and messaging and e-mail on the move on your mobile and so on. There is a tendency to try and cram more and more stuff into those small devices so clearly when that device falls prey to an attack then the ability to unravel all of your personal details, capture all of your contact details, read all of your messages, possibly connect back to your home networks, that becomes fairly significant. We did mention Wi-Fi insecurity. Again these devices are becoming increasingly connectable. It concerns me that in the protocols being used we do not seem to be learning the lessons and every time a new product comes along that has a new wireless connectivity mechanism they seem to make the same mistakes. They reinvent the security mechanisms, the crypto or whatever. With WEP they invented a whole new crypto tracking system to secure those networks and got it wrong. Bluetooth came along and they invented their own crypto system and again got it wrong and are now having to generate new ones. So we do not seem to be learning the lessons of the previous generations of communication. The

Internet has been doing secure communications for years and then suddenly we are on wireless and then we have to reinvent secure communications which we should not have needed to. We could have learned the lessons from the Internet and applied them to wireless.

Q331 ***Lord Harris of Haringey:*** So you not saying for example mobile phones are inherently secure; you are saying it is a failure to learn the lessons of the past?
Mr Laurie: And the failure to secure them has much greater effect now because of how they are being used. For Microsoft we talked about single identity and if your mobile phone becomes the device that is your identity it will contain the credentials of your identity and maybe biometrics. We see laptops with fingerprint readers and so on. There is an increasing reliance on technology to solve these problems like identity, but because they not getting the security right the threat becomes much greater. If I can take over your entire identity by stealing the contents of you mobile phone which now has a single sign-on ID and your biometrics, fingerprints, iris scans, whatever, then that is a huge problem. I think the risk of that happening is increasingly there because of this reliance on new technology just working and we will get it right.

Q332 ***Lord Harris of Haringey:*** Do you feel that manufacturers are doing anything like enough to address these problems?
Mr Laurie: I think they are trying but history shows us that they tend not to get it right, so I guess the simple answer to that is probably not.

Q333 ***Lord Harris of Haringey:*** Do you have any information about the scale of the problem in terms of the number of times or number of instances where the attack has been through a mobile device as opposed to more conventional means?
Mr Laurie: I do not have any data relating to current situations but certainly in the past for example when I looked at Bluetooth issues and found vulnerabilities in the Bluetooth protocol, what I found was there were huge numbers of people who were vulnerable. I did some scans of Victoria Station during rush hour, and from memory I think I found about 350 vulnerable phones in the space of about an hour, and that was transitory people who were walking past, that was not the same person being counted multiple times. These technologies are being shipped in their hundreds and thousands and millions, so if there is a vulnerability of a mobile device that spreads very quickly, there will be a lot of them out there.

Q334 ***Lord Howie of Troon:*** How did you find these vulnerable devices?
Mr Laurie: Bluetooth has a facility to scan for other Bluetooth devices. I was simply scanning, I was not attacking them, and I was looking at the profile to say, okay I recognise that profile as being a particular device that is known to be vulnerable.
Lord Harris of Haringey: Before we move on, it may be that is something we should be seeking specific evidence on from particularly providers and suppliers of equipment as to what they are doing to address the vulnerabilities of mobile devices. It is a component of the area we are looking at but I am not sure we have hard evidence and have specifically asked about mobile phones.

Q335 ***Chairman:*** If mobile devices were enabled by a fingerprint scan or an iris scan, the fact you had the file for the iris scan or the fingerprint scan would not help you, or can you inject a signal into the machine and mimic it?
Mr Laurie: The potential is there. If you know the fingerprint you are trying to spoof then you have got the pattern you are trying to create, so you can generate a fake fingerprint that will fool that reader. It has long since been proved that most fingerprint readers on the market are actually vulnerable to very simple attacks. In fact, there is a kids' TV programme called *Mythbusters* where they recently tried a fingerprint reader and they defeated it in three different ways, one of which was a simple photocopy of the fingerprint, and this was one that the industry was saying this is foolproof.

Q336 ***Chairman:*** Is that by making an imitation fingerprint or by injecting an electronic signal?
Mr Laurie: This was by making an imitation fingerprint. It is all very James Bond but you collect a fingerprint from a glass or a CD case. I think in the case of the programme they lent the guy a music disk and when they got it back they took the fingerprint off the outside of the case and recreated that as a photocopy.

Q337 ***Chairman:*** Soon you will be able to buy a little fingerprint printer, will you?
Mr Laurie: Absolutely. The tools are all out there. This is not a problem.

Q338 ***Lord O'Neill of Clackmannan:*** I am almost loath to ask this question because you have frightened us enough as it is! Looking to the future what do you see as the most important emerging security threats in respect of personal safety?
Mr Laurie: I slightly jumped the gun there because that was one of the main things that concerns me the most—the reliance on biometrics. Single centralised databases of personal information—the more that we gather this stuff together in one place the more vulnerable we make ourselves and the easier we make

it for people to take over our identities. Again it is the reliance on technology. If you spend millions on systems that say biometrics are foolproof and we are going to use these biometrics to prove our identities and we have spent lots of money on it and it is foolproof, that causes a real problem for somebody caught up in the system when their identity has been spoofed. How do I convince this huge industry that they have got it wrong? There is a serious inertia against admitting that there is a problem with the system so the more you claim a technology is foolproof and the more money you spend on it the harder it gets to show they were wrong.

Q339 ***Chairman:*** Do you think that ID cards will be vulnerable in the same way?
Mr Laurie: Definitely. History tells us that these technologies are not foolproof. I have done some work in the area of RFID and there are lots of cases where industry is claiming that an RFID cannot be cloned for example—

Q340 ***Lord Mitchell:*** What is an RFID?
Mr Laurie: Radio frequency identification, so for example in your new passport if you have a passport that is issued since October it will have a chip in it and the chip contains some biometric information. At the moment it is just the photograph and the data that is printed on the inside of your passport, but in the future the plans are to also have fingerprints, iris scans, possibly a scan of your birth certificate that was used to prove your identity in the first place. This is the same technology that is going to be used in the ID card. It has already been demonstrated that those chips in the passports can be cloned, so part of the reason for putting them in the passport in the first place was to improve the security of the passport and yet here we are, they have only been deployed since October and there are already people making copies of them.

Q341 ***Lord Harris of Haringey:*** Yes, but you would still have to be in possession of the right fingerprints when you appeared at the point of entry.
Mr Laurie: If the passport has an image of that fingerprint in it and I can skim the passport from your pocket. The point about an ID card is that you can read the data on it without physically having it on your hand. You have to be within a couple of inches.

Q342 ***Chairman:*** It is like an Oyster card?
Mr Laurie: Exactly, that is RFID.

Q343 ***Chairman:*** It is like a ski card, they have had them for years.
Mr Laurie: Exactly.

Q344 ***Lord O'Neill of Clackmannan:*** Can I get this right, what is the point of having any security at all if you are going to be able to rip it off at every turn? You guys are great at telling us what is wrong but you never give us any solutions because it seems that one of your other colleagues is trying to work out how to rip off the next generation. I am not associating you with them but people in your line of country. What do we do then, just give up?
Mr Laurie: No, not at all. I think the problem is appropriate use of technologies.

Q345 ***Lord Sutherland of Houndwood:*** On that can I ask you a) do you have a mobile phone—and you clearly do because you were scanning at Victoria Station—and b) do you have protocols that you operate yourself to ensure that this thing is not vulnerable in the way that you are scaring the wits out of us?
Mr Laurie: Most of us in the open source security industry apply our own level of security over and above that which would be deployed in the normal systems.

Q346 ***Lord Sutherland of Houndwood:*** Are these technical or behavioural?
Mr Laurie: Both.

Q347 ***Lord O'Neill of Clackmannan:*** Do they derive from paranoia? All paranoia is based to an extent on persecution of a genuine character, but is life maybe not too short?
Mr Laurie: I think healthy paranoia is good. As I said, it is putting too much reliance on a new technology. It is fine if you treat it in the appropriate manner. If you think these chips are going to be out there for 10 years, what system have we got currently that was invented 10 years ago, was issued over a secure system and is still secure now?

Q348 ***Chairman:*** You still have to produce your finger and put it on a fingerprint scanner. I do not agree with you.
Mr Cox: Unfortunately, remember we said earlier you can make copies of fingerprints. The fingerprint is also on the chip. I assume the Passport Office use very high quality ones but to fool a fingerprint scanner all I end up needing to make is a small piece of plastic that fits over the end of my finger which is almost invisible.
Mr Laurie: It all sounds very James Bond but it is actually very easily doable and demonstrably so.
Mr Cox: You can make it with a laser printer, PVA glue and a couple of printer's tools. That is all it needs.

Q349 ***Chairman:*** There would be ways around that would there not if you could inspect people's fingers! Let me go on to the last question and that is addressed to you Mr Laurie again because you have drawn attention in the past to the fact that discarding aeroplane boarding card stubs does contain frequent flier data which could result in identity theft. You also note in your evidence that airline websites can leak personal data to hackers. What can be done to ensure that businesses take their responsibility for the security of our personal data seriously? Should businesses such as airlines be legally liable for individual losses in such circumstances?
Mr Laurie: I guess first of all I should say that airlines were merely a case in point here and they are no more likely to leak data than any other website that collects data. It just happened to be the case that I was looking at that particular scenario. However of course, the data that they are collecting is particularly sensitive because it is things like date of birth and passport number and so on. They already have a duty of care under the Data Protection Act to look after that data so I think we already have regulation that should be compelling them to look after it properly. The question I guess is when there is a breach and when the data is leaked how one gets to know that one's data has been leaked or what penalties there are against them if it does not end up going to court and they are being prosecuted. Potentially one of the things we could look at is the system that they have adopted in California (quite a few states have adopted it now but California was the first) which is that if a company loses personal data they have to disclose publicly that they have done so, they have to notify the person affected that their data has been lost. When I say disclosed publicly they have to inform the state press; here it would obviously be the national press. So you are using PR as a tool against them, they get bad publicity for having bad security and they are then much more likely to take the next case much more seriously.

Q350 ***Chairman:*** Is it your opinion that we should have the same laws here?
Mr Laurie: I think we should.
Chairman: Thank you both very much. I don't think you have cheered us up, but you have informed us a great deal, so thank you very much, we appreciate your time.

WEDNESDAY 24 JANUARY 2007

Present	Broers, L (Chairman)	Patel, L
	Erroll, Earl of	Sharp of Guildford, B
	Harris of Haringey, L	Sutherland of Houndwood, L
	Hilton of Eggardon, B	Young of Graffham, L

Memorandum from the Society for Computers and Law—Internet Interest Group and Privacy and Data Protection Interest Group

Introduction

1. The Society for Computers and Law was created in 1973 to encourage and develop IT for lawyers and IT-related law. Lord Saville is the Society's President. The Society is, literally, "Where Computers and Law meet", and provides a forum for members to meet and exchange information and ideas or raise issues of concern with others. Through its membership, its widely acclaimed magazine Computers & Law, regional meetings and national conferences, the Society promotes issues of importance to both IT Law and the implementation of IT within legal and related practices.

2. The Society for Computers and Law welcomes this opportunity to respond to the House of Lords Science and Technology Committee Call for Evidence and to contribute to the important debate concerning personal Internet security.

3. We understand personal Internet security to be about the information security and integrity of private domestic end-users' systems, networks and other terminal devices accessing the Internet via the publicly available services of electronic communications service providers. We recognise that such access is principally achieved in the UK by end-users obtaining the services of a fixed electronic communications network Internet Services Provider (ISP). However, the Society recognises that the development of mobile telecommunications such as "2.5G", Edge and 3G, together with other wireless access technologies such as WiFi and WiMax, will have an increasing impact on the way end-users obtain access to the Internet.

4. The Society for Computers and Law is the major UK organisation for IT lawyers. It has over 1,600 members and includes within its membership the leading IT lawyers from the various UK jurisdictions as well as leading members of the legal profession with an interest in IT law. The Society is not however a trade association or survey body and we cannot therefore produce our own statistics or analyses of trends to support our views set out in this response. However, we hope our views, which have been prepared by a committee of our members, assist the Committee in its consideration of this important topic. We will set out our views against the questions set by the Committee in its Call for Evidence, where appropriate.

Defining the Problem

What is the nature of the security threat to private individuals? What new threats and trends are emerging and how are they identified?

5. We believe that the Internet does not provide any new threats to citizens in terms of endangering citizens in new ways. Instead, we consider that the Internet merely facilitates the commission of a larger and broader range of "traditional" crimes by the criminally-minded. For example, whilst "identity theft" as defined by the Home Office Identity Fraud Steering Committee[1] may not of itself be a criminal act, dishonest use of identity information to obtain property would be theft under the Theft Act 1968, even before considering potential offences under the Computer Misuse Act 1990 for any unauthorised access to a computer to obtain the relevant identity information.

6. We recognise, however, that certain criminal activity that was prior to the Internet relatively controlled, such as the distribution or possession of child pornography (offences under section 1(1)(b) and (c) of the Protection of Children Act 1978), has exploded with the ease of access to child pornography facilitated by the Internet.

[1] see the definitions at http://www.identity-theft.org.uk/definition.htm

What is the scale of the problem? How are security breaches affecting the individual user detected and recorded?

7. We have no independent research on these matters. However, for a recent analysis of threats and their prevalence, we commend to the Committee the research carried out by the BBC reported during the week 9–13 October 2006[2] and the research of the Honeynet Project[3].

How well do users understand the nature of the threat?

8. Whilst we do not have any statistics to back our assertion, we feel that there is a low level of understanding of both the threats posed to end-users by the Internet and the tools available to end-users to protect themselves. We suspect that it is this general ignorance that is feeding the high level of fear that end-users are reporting in surveys about Internet use (for example, the survey reported by the Government's Get Safe Online initiative on 9 October 2006 stating that 21percent of a survey of users feared "e-crime" more than mugging, burglary or car crime.[4]

Tackling the Problem

What can and should be done to provide greater computer security to private individuals? What, if any, are the potential concerns and trade-offs?

9. In our view there are only three groups that can have an impact on computer security for private individuals: end-users themselves, ISPs/Internet access providers and manufacturers/suppliers of terminal devices and software. Taking each in turn:

End-users

- We believe that there is a requirement for greater education of users about the security threats posed to them by the Internet and the potential solutions that are available to them for self-protection. Whilst we support initiatives such as the Government's Get Safe Online, we are concerned that education alone is not a sufficient response, given the fact that providing consumer advice and information does not always appear to be effective. Many consumers appear to be inefficient at implementing the technical protection measures that are available to them, even when they are aware of the general security risks.
- We note the experience of MasterCard International in the United States of America, which reported a security breach to the Federal Bureau of Investigation on 17 June 2005 and subsequently went public on the breach. We are not aware of consumers cancelling MasterCard credit cards in significant numbers after the breach was publicised. We therefore consider that, even when consumers are presented with the relevant information, they do not necessarily respond in the way one might expect, and which might be desirable or even essential.

ISPs

- Given that we consider that educating end-users may have a limited effect on increasing the level of security and Internet integrity in the UK, we believe that the group most able to influence the levels of personal Internet security are the ISPs or other Internet access providers. We consider that close examination should be given to whether an obligation on ISPs to implement access controls and technical security measures could be expected to reduce the security risks, and whether this could be done cost-effectively.
- However, if ISPs were required by some form of intervention to improve the access controls and technical security measures included within their services, there is an argument that this would restrict consumer choice and would unnecessarily increase the cost of Internet access in the UK.
- Free market advocates argue that there is adequate choice in the market; for example, consumers with security concerns can choose an ISP that provides a high level of security protection with its access services, such as AOL (UK) Limited (which provides parental controls for access to content as well as advice and McAffee® security software), at a slightly higher cost than services that provide access only—a non-exhaustive list of broadband ISPs in the UK is maintained by ADSLguide.org.uk[5] Whilst we acknowledge the free or open market arguments concerning consumer choice, we are also aware that unlimited choice for one user does affect other Internet users

[2] see http://news.bbc.co.uk/1/hi/technology/default.stm
[3] see http://www.honeynet.org/misc/project.html
[4] see http://www.getsafeonline.org/
[5] at http://www.adslguide.org.uk/isps/summarylist.asp

and society as a whole. For example, users with unprotected PCs who choose to obtain access via an ISP that has no controls or security measures are more likely to be attacked by botnet herders, who can then expand their botnet to the detriment of all other (protected/secure) users of the Internet and to the public, if such botnets are used for criminal purposes.[6] Regulating for minimum levels of security protection can be argued to be the Internet equivalent of requiring all drivers to wear seatbelts—it is an infringement of drivers' liberty, but for the mutual benefit of all road users and society at large.

Terminal Devices Manufacturers/Software Suppliers

— As stated above, we consider that the group most able to improve Internet security are the access providers. However, we also see that manufacturers of hardware and suppliers of hardware and software have a role to play in supporting ISPs, as indicated in this response below. We also consider that a simple and voluntary labelling system, similar to the Food Standard Agency's "traffic light" system, could be considered to identity those hardware and software products that have "high", "medium" and "low" levels of protection against particular classes of security threat.

We consider that a number of steps could be taken to improve personal Internet security, as follows:

National High Tech Crime Unit

— We consider that the disbanding of the UK's only body exclusively and publicly tasked with investigating crimes related to Internet security was a retrograde step. Whilst we understand that the expertise developed by the National High Tech Crime Unit will not be lost by its integration into the Serious Organised Crime Agency, we believe that the expertise may be diluted over time as SOCA's emphasis on organised crime takes precedence. We also consider that the National High Tech Crime Unit provided a useful source of public information and guidance on Internet security issues.

"Opt Out" Security

— We consider that it should be industry-practice that, where a terminal device or software program is supplied to a private consumer, it is supplied with the default security settings and any parental or other controls on the device or in the software turned on, with suitable guidance and warning to end-users on the risks associated with reducing the security settings.

Minimum Security Standards

— We believe that relevant electronic communications network and services providers should be required to ensure minimum standards of security and network integrity. In particular, we consider that ISPs should maintain minimum security levels for their community of users. We propose that amendments to existing electronic communications law and regulation can implement such minimum standards, as set out below.

What is the level of public awareness of the threat to computer security and how effective are current initiatives in changing attitudes and raising that awareness?

10. We have no independent research on this question.

What factors may prevent private individuals from following appropriate security practices?

11. Again, we have no independent research we can offer the Committee on this question. However, we suspect that the complexity of many security options may be a factor, which is one of the reasons why we recommend an "opt-out" security approach.

What role do software and hardware design play in reducing the risk posed by security breaches? How much attention is paid to security in the design of new computer-based products?

12. We believe that an "opt out" regime for optional security measures should be implemented. We consider that there are adequate software and hardware solutions to the most common security threats, with a thriving market in the development of solutions to meet new threats.

[6] for a useful glossary of these and other computer security related terms, see the BBC website at http://news.bbc.co.uk/1/hi/uk/5400052.stm

Who should be responsible for ensuring effective protection from current and emerging threats?

13. As indicated above, we consider that responsibility should be shared between end-users, ISPs and software/hardware manufacturers/suppliers.

What is the standing of UK research in this area?

14. We have no information to be able to answer this question.

Governance and Regulation

How effective are initiatives on IT governance in reducing security threats?

15. Whilst we cannot quantify the usefulness of Government initiatives, we believe they are an essential part of educating end-users in the risks and promoting the adoption of appropriate security precautions and safe Internet use. Co- and self-regulatory initiatives, where Government look to industry to bear the burden of regulating for good practice, should be encouraged wherever possible.

How far do improvements in governance and regulation depend on international co-operation?

16. Whilst the nature of the Internet requires international co-operation, we consider that there is value in the UK considering the implementation of regulation to improve the quality and quantity of security protection measures in the UK. The Internet Watch Foundation (www.iwf.org.uk) is an example of an industry funded model of self-regulation that has successfully removed specific types of illegal content from being hosted within the UK and limiting access to such material when sourced from foreign jurisdictions. We consider that whilst a "fortress UK" is not technically feasible, or indeed desirable, we believe society and the UK online business economy would benefit from a more secure community of Internet Service Providers and users.

Is the regulatory framework for Internet services adequate?

17. We consider that the existing regulatory framework under Regulation 5 of the Privacy and Electronic Communications Regulations 2003 (the ePrivacy Regulations), which implements Article 4 of the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (the ePrivacy Directive), is only an adequate starting point for the regulation of security for Internet services. For ease of reference, Regulation 5 is set out below:

Security of public electronic communications services 5:

(1) Subject to paragraph (2), a provider of a public electronic communications service ("the service provider") shall take appropriate technical and organisational measures to safeguard the security of that service.

(2) If necessary, the measures required by paragraph (1) may be taken by the service provider in conjunction with the provider of the electronic communications network by means of which the service is provided, and that network provider shall comply with any reasonable requests made by the service provider for these purposes.

(3) Where, notwithstanding the taking of measures as required by paragraph (1), there remains a significant risk to the security of the public electronic communications service, the service provider shall inform the subscribers concerned of-

- the nature of that risk;
- any appropriate measures that the subscriber may take to safeguard against that risk; and
- the likely costs to the subscriber involved in the taking of such measures.

(4) For the purposes of paragraph (1), a measure shall only be taken to be appropriate if, having regard to:

- the state of technological developments, and
- the cost of implementing it.

it is proportionate to the risks against which it would safeguard.

(5) Information provided for the purposes of paragraph (3) shall be provided to the subscriber free of any charge other than the cost to the subscriber of receiving or collecting the information.

18. Our difficulty with the ePrivacy Regulations is that no guidance or standards are included in either the ePrivacy Regulations or the ePrivacy Directive on what appropriate technical and organisational security measures may be. We are also concerned that enforcement of Regulation 5 is, by Regulation 32, by the Information Commissioner. We comment on enforcement of the Data Protection Act 1998 below. For the same reasons, we do not consider that the Information Commissioner is the proper person to enforce this provision. We believe that this should be a matter for Ofcom.

19. The Communications Act 2003 (the Act) could be used to implement Article 4 of the ePrivacy Directive and the minimum security levels we propose. Ofcom has a duty under section 3(1)(a) of the Act to further the interests of citizens in relation to communications matters. It also has the power to set general conditions of entitlement to provide an electronic communications network or service under section 45(1) of the Act.

20. The current General Conditions of Entitlement were published in accordance with section 48(1) of the Act by Oftel on 22 July 2003.[7] They include, at Condition 2, conditions relating to communications providers' compliance with compulsory standards or specifications, largely concerned with network interfaces, services compatibility and interconnection. They also include, at Condition 3, a requirement that providers of fixed public telephone networks and/or publicly available telephone services, amongst other obligations, take all reasonable practicable steps to maintain to the greatest extent possible the proper and effective functioning of the fixed public telephone network. We propose that consideration be given to including in the General Conditions of Entitlement a condition in the same terms as Regulation 5 of the ePrivacy Regulations or Article 4 of the ePrivacy Directive and to require adherence to the appropriate security standards. A draft new General Condition of Entitlement is included in Annex A to our response.

21. In determining what appropriate security standards may be applied by Ofcom, we suggest that consideration should be given to BS:7799 (now BS ISO/IEC 17799:2005) "Information technology—Code of Practice for Information Security Management" as an appropriate internationally recognised security audit standard and ISO/IEC 27001:2005 "Information technology—Security techniques—Information security management systems" as being appropriate standards to which communications providers should be certified. However, we note that the generic form of Condition 2 of the General Conditions of Entitlement, as amended in our proposed new General Condition, can take into account all appropriate international standards.

What, if any, are the barriers to developing information security systems and standards and how can they be overcome?

22. A significant barrier to the universal adoption of secure information systems is cost (or perceived cost). As a Society we are not in a position to be able to quantify what the costs to ISPs would be of implementing ISO/IEC 27001:2005 compliant Internet access, or what this would amount to as an additional cost per subscriber or end-user.

23. Whilst there will be a cost to network and services providers, which may be passed on to end-users, of adopting minimum information security systems and standards, any additional costs incurred by Ofcom in policing a new General Condition can be recovered by the fees provisions of the Act.

Crime Prevention

How effective is Government crime prevention policy in this area? Are enforcement agencies adequately equipped to tackle these threats?

24. We have no independent measure of effectiveness. However, we are concerned that expertise concentrated in the former National High Tech Crime Unit may be dissipated and lost. Whilst we are also concerned that there may be a reluctance within the Crown Prosecution Service to pursue criminal charges where the only charges available are those under the Computer Misuse Act 1990 or the Data Protection Act 1998 for computer related crime, we recognise that charges for offences under these Acts are brought where the criminal behaviour in question allows other offences to be charged at the same time.

25. We consider that the penalties, criminal sanctions and enforcement provisions of the Data Protection Act 1998, together with the resources made available to the Office of the Information Commissioner, continue to be inadequate to address the other side of personal Internet security—the misuse of personal data. In particular, we note that the obligations on data controllers to protect personal data with appropriate technical and organisational measures (the seventh data protection principle at Part 1 of Schedule 1 to the Data

[7] see http://www.ofcom.org.uk/static/archive/oftel/publications/eu—directives/2003/cond—final0703.pdf

Protection Act 1998) are not rigorously enforced. We are not aware that there has been any enforcement by the Information Commissioner, whether at the request of Ofcom or otherwise, of Regulation 5 of the ePrivacy Regulations. We believe that the only way the Office of the Information Commissioner will be able to enforce the Data Protection Act 1998 effectively is if it is given the power to levy penalties on defaulting data controllers, which it would be entitled to retain to fund its enforcement operations. However, as stated above, we believe Ofcom should have the responsibility for enforcing Regulation 5 of the ePrivacy Regulations.

26. One problem is the lack of reporting by those that have suffered a security breach. One mechanism to address such non-reporting would be the imposition of a legal obligation on organisations to report incidents of security breach. Since 2003, for example, the Civil Code of the State of California has obliged private businesses and public agencies to report if they have suffered "a breach of the security" of a system that contains personal information, including financial data.[8] The stated purpose of the statute was to tackle the growing problem of "identity theft", but it is also recognition that the data processed by an organisation often engages the private interests of individuals, as subjects of the processed data, as well as public interests which may not coincide with the private interests of the victim organisation. Such a measure is an obvious complement to the imposition of obligations to implement data security measures, under data protection law. We note that the European Commission is considering such a breach notification requirement in its proposed amendments to the ePrivacy Directive[9], with the proposed notification obligation being both to report breaches to the relevant national regulatory authority and to the affected data subjects. The consultation period on these proposed amendments expires on 26 October 2006. We also note that these proposals have recently been endorsed by the Article 29 Working Party established under the European Union Data Protection Directive 95/46/EC[10]. We suggest that consideration should be given to an amendment to the ePrivacy Regulations for breach notification.

Is the legislative framework in UK criminal law adequate to meet the challenge of cyber-crime?

27. To date the current criminal law appears to have been effective in being able to be applied to cyber-crime, given that in a majority of circumstances the Internet merely provides a modern tool to those intent on committing established offences. Where problems have arisen, or lacunae exposed, the courts or Parliament have been able to adequately address the issue through judicial interpretation or statutory amendment. The courts have also begun to apply the Computer Misuse Act 1990, prior to its forthcoming amendment, sensibly.

How effectively does the UK participate in international actions on cyber-crime?

28. This is a matter outside the Society's experience.

Conclusion

29. In conclusion, our recommendations are that:

- Communications providers be regulated by Ofcom to ensure that minimum standards of information security or network integrity based on industry/internationally recognised standards are adopted;
- Hardware and software that incorporate security or other protection measures should be distributed to consumers with the security functionality 'turned-on', as the default setting for such hardware and software;
- The National High Tech Crime Unit be reformed;
- The resources for enforcement of the seventh data protection principle (the obligation for data controllers to implement appropriate technical and organisational measures for the security and integrity of personal data) be increased, possibly by a self-funding mechanism from the levying of increased penalties for breach of the principle; and
- Data controllers should be subject to an obligation to notify security breaches to the data subjects whose data has been compromised, as well as to the Information Commissioner.

23 October 2006

[8] Similar legislation has been adopted in 22 US states.

[9] http://europa.eu.int/information—society/policy/ecomm/doc/info—centre/public—consult/review/staffworkingdocument—final.pdf

[10] see http://ec.europa.eu/justice—home/fsj/privacy/docs/wpdocs/2006/wp126—en.pdf

Annex A

PROPOSED NEW GENERAL CONDITION OF ENTITLEMENT (PURSUANT TO SECTION 45(1) OF THE COMMUNICATIONS ACT 2003)

1. The following is a draft of a new information security and network integrity General Condition of Entitlement. It replicates the obligations already placed upon service providers by Regulation 5 of the Privacy and Electronic Communications Regulations 2003, but by making them a General Condition of Entitlement they can be enforced by Ofcom. In addition, the Condition includes obligations to take into account appropriate standards and specifications, using paragraphs that are near identical to those in Condition 2 of the General Conditions of Entitlement.

Information Security and Network Integrity

2. The Communications Provider shall take appropriate technical and organisational measures to safeguard the security of its Public Electronic Communications Services and the security and integrity of End-users' equipment used in connection with those Public Electronic Communications Services.

3. If necessary, the measures required by paragraph 2 may be taken by the Communications Provider in conjunction with the provider of the Electronic Communications Network by means of which the Public Electronic Communications Service is provided, and that Electronic Communications Network provider shall comply with any reasonable requests made by the service provider for these purposes.

4. Where, notwithstanding the taking of measures as required by paragraph 2, there remains a significant risk to the security of the Public Electronic Communications Service or the security and integrity of End-users' equipment used in connection with those Public Electronic Communications Services, the Communications Provider shall inform its End-users of-

(a) the nature of that risk;

(b) any appropriate measures that the End-user may take to safeguard against that risk; and

(c) the likely costs to the End-user involved in the taking of such measures.

5. For the purposes of paragraph 2, a measure shall only be taken to be appropriate if, having regard to:

(a) the state of technological developments; and

(b) the cost of implementing it.

It is proportionate to the risks against which it would safeguard.

6. Information provided for the purposes of paragraph 4 shall be provided to the End-user free of any charge other than the cost to the End-user of receiving or collecting the information.

7. The Communications Provider shall ensure that any restrictions imposed by it on access to and use of a Public Electronic Communications Service on the grounds of ensuring its compliance with paragraph 2 above are proportionate, non-discriminatory and based on objective criteria identified in advance.

8. The Communications Provider shall take full account of any relevant voluntary standards and/or specifications adopted by the European Standards Organisations in assessing the appropriateness of any measure for the purposes of paragraph 2 or, in the absence of such standards and/or specifications, international standards or recommendations adopted by the International Telecommunication Union (ITU), the International Organisation for Standardisation (ISO) or the International Electrotechnical Committee (IEC).

9. In the absence of such standards and/or specifications referred to in paragraph 8 above, the Communications Provider shall take full account of any other standard specified by Ofcom in a direction under this Condition to define appropriate technical or organisations measures, provided that Ofcom shall not make such a direction if an appropriate European or other international standard is expected to be promulgated within a reasonable time.

10. For the purposes of this Condition:

(a) "Communications Provider" means a provider of a Public Electronic Communications Service; and

(b) "European Standards Organisations" means the European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (CENELEC), and the European Telecommunications Standards Institute (ETSI).

Memorandum by the Information Commissioner's Office

1. The Information Commissioner welcomes the inquiry by the Science and Technology Committee into personal Internet security. The Commissioner shares the concern that Lord Broers expresses. Whilst we are increasingly doing more and more online all too many of us do not fully appreciate the risks. The Commissioner is not submitting detailed evidence on the nature of the risks, and appropriate counter measures, because there are others better placed to provide authoritative evidence on these matters.

2. The problems of educating citizens regarding the risks are highlighted by the dangers of using file-sharing software. This can mean that information and documents held on a computer can be accessed remotely. The practical dangers are all too obvious. Someone may use their home computer to prepare some documents for work purposes, unaware that someone else in the household has downloaded file-sharing software. This can put sensitive information and documents at risk. Whilst employees may have been warned about the dangers of using a home computer for work purposes, the fact that many of us do not have a full appreciation of the nature and extent of the potential risks can lead even those who are normally cautious to put sensitive information at risk. Even if a home computer is only used for domestic purposes, if file-sharing software is installed this can result in sensitive private information being put at risk.

3. However, the dangers of file-sharing software have been known about for some years. For example, in November 2003 *The Guardian* published a detailed article on the use of this software, particularly for sharing images of the sexual abuse of children. Moreover, those providing popular file-sharing software, such as LimeWire and Kazaa do warn users of the risks and of the need to be careful in selecting which folders they are happy to share. Nevertheless, many of those who install this software do not take the necessary precautions. This raises the question of whether the mechanisms for ensuring safe use are simple enough for those who are not particularly IT literate to understand and use.

4. The Commissioner believes, therefore, that there is a real need to ensure that all of us who use computers are aware of the risks and the steps we can take to minimise those risks. The task of education is a shared one, schools, parliament, government, employers, regulators and especially industry, all have a part to play. There is a risk that, regardless of concerted efforts to educate, there will be those who believe that such matters as Internet security are just too technical for them. The Commissioner considers, therefore, that great emphasis should be placed on ensuring that privacy and security-friendly use of the internet is as straightforward as possible. This may well require industry to reconsider whether their products are as easy to use safely as they could be and whether more can be done to design in a safety first approach.

24 October 2006

Examination of Witnesses

Witnesses: MR NICHOLAS BOHM, The Law Society, PROFESSOR IAN WALDEN, Society for Computers and Law, and MR PHIL JONES, Assistant Commissioner, Information Commissioner's Office, examined.

Q351 ***Chairman:*** Mr Bohm and Mr Jones, thank you very much for joining us today. We are going to proceed although Professor Walden is not here because there are certain questions which are more addressed to you and I think it will be more efficient that way. He is giving a lecture, evidently, and may be a bit late. You should be aware that we are being webcast and televised today. For any member of the public here, there is an information note for you, which you may have picked up already. We can start first by you introducing yourselves, if you would, and then if you wish you can make an opening statement or we will go straight into questions. Shall we start with you, Mr Bohm?

Mr Bohm: I am Nicholas Bohm. I contributed to the submission to the Sub-Committee made by the Foundation for Information Policy Research and I am also a member of the Law Society's Electronic Law Committee. This area has been a field of interest for some years. I do not think I need to make an opening statement of any kind. I am happy to deal with questions along the lines indicated, or indeed any others.

Mr Jones: I am Phil Jones. I am an Assistant Commissioner of the Information Commissioner's Office. The Information Commissioner is responsible for promoting and monitoring compliance with the Freedom of Information Act, the Data Protection Act, and more relevant to today's circumstances the Privacy and Electronic Communications Regulations. Again, I do not have any opening statement to make.

Q352 ***Chairman:*** Thank you very much. Let me go into the first question. Who should most appropriately carry the risk of on-line fraud, and are statutory changes needed to achieve this?

Mr Bohm: The basic legal position is that if fraud consists of misrepresentation—and in the on-line context normally it does—then the person who is deceived by the misrepresentation is the one who *prima facie* carries the loss. That position is part of

the common law notion that a claimant must prove his case, so that if someone seeks to hold me to a bargain which he says I made and I say "I did not make it, it was someone pretending to be me", he has to prove it was me in order to prove his case; and if he cannot prove it was me, then he stands the resulting loss. He may have a claim against the person by whom he was deceived, but as between him and me he bears the loss and he tries to recover it somewhere else if he can. The common law position has occasionally been buttressed statutorily and the written submission refers the Sub-Committee to the Bills of Exchange Act where in the late nineteenth century the common law was codified so that a forged cheque is a nullity and there is no way the bank can debit your account with it; it lacks authority. That has not generally been codified. Where codified, it is irreversible by contract; where it is not codified, it can be reversed by contract. So you can have contracts under which, for example, a bank might seek to say, "If your password has been used in an on-line transaction, then we are authorised to debit your account whether you were the person who used it or not. So even if we were deceived by a third party, you stand the loss." That would be attempting to shift the risk by contract. The only existing defences against attempts to shift the risk by contract are the Unfair Contract Terms Act and the regulations made under the European Directive which points in the same direction. That is how one would argue if one was faced with a contract term of that kind and there had been a fraud. I think the common law position leaves the risk in the right place, that is to say those who deploy security systems for the purpose of checking that the customer is the one making the transaction are the ones who should stand the risk of it failing. They mostly at the moment deploy systems which are inherently weak because they are based on shared secrets. When your bank asks the caller for my mother's maiden name it is hardly a reliable method, and if the bank chooses to rely on it and it does not work it should be the bank's problem, not mine. So I think that consumers in particular probably need a bit of support in achieving the position of being free from this risk. If a bank says, "No, our system is perfect. We know it must have been you or somebody you gave the number to," consumers can have a bit of a hard time in establishing what ought to be for the bank to prove the other way. I would like to see the banking system Ombudsman, the Office of Fair Trading and anybody else concerned with unfair contract terms encouraged to take a robust line, but I think the law points in broadly the right direction as it is.

Q353 ***Chairman:*** Thank you. Before we proceed, welcome, Professor Walden. We decided to go ahead because the early questions are more orientated towards the other two, but thank you for being here. Would you like to just introduce yourself for the record?
Professor Walden: Yes. First, let me apologise. I had the typical problem of trying to get through security in time. My name is Professor Ian Walden. I am head of the Institute of Computer and Communications Law at Queen Mary University of London.

Q354 ***Chairman:*** Thank you. Would you like to say anything as an opening statement, or are you happy that we proceed?
Professor Walden: I am happy to proceed.

Q355 ***Chairman:*** Did you have anything to add, Mr Jones?
Mr Jones: I have nothing to add because I should point out that I am not an expert in fraud and the important point is that the rules for which our office is responsible which relate to unsolicited marketing communications relate to those as being unsolicited. Whether they are deceptive, misleading, potentially fraudulent does not really matter; it is an issue of whether they are unsolicited or not.

Q356 ***Chairman:*** The banks are currently reimbursing people who lose money to phishing scams, for example. However, losses are currently small in the context of overall banking turnover and should losses rise significantly there is no guarantee that the banks will continue this policy. Should such reimbursement be a legal requirement, in your opinion?
Mr Bohm: Yes, I think that it should be. I think the banks are deploying the systems and if they are not effectively and securely useable by their customers then the loss should clearly be on the banks, and I think the law should be a little more categorical in the customer's support than it is as matters stand. I think phishing is very difficult to deal with because if customers can be deceived into believing that they are dealing with a bank by someone who manages to stand in the middle between them, then whatever security mechanism is operating between the bank and the customer, they are both being deceived into passing security secrets through the middleman. But banks up to now have simply not been very good at enabling customers to be sure they are dealing with the bank and not a crook. Too many banks will still telephone a customer and then say, "But in order to discuss what I am ringing you up about, I must ask you to give me your security details," which is training the customer to give to an unknown person their security details. It is a very undesirable procedure. The better ones have a script for how to deal with a customer who raises this point and the poorer ones do not even have a script, but actually none of them should ever do it in the first place. Some

banks still send out emails with clickable links in them, which is exactly the same error of training the customer to go through an insecure procedure. What the bank should be doing is helping the customers to understand how to be sure that it is the bank they are dealing with before they part with their secrets. I do not see very much sign of that at the moment. If the volume of phishing fraud rises, the incentive to get those things right needs to fall firmly on the banks and I think it is an incentives question.

Q357 ***Chairman:*** Do you think that the services available to people who have a complaint against the bank are adequate in these cases? Are the ombudsmen, if they exist—and perhaps you could talk a bit about that—sufficiently independent of the banks?
Mr Bohm: I think they are probably sufficiently independent, but when I last looked at a series of the Ombudsman's deliberations on the subject of what were then called "phantom withdrawals" from cash machines I had the impression that the Ombudsman's approach was not very sophisticated, not very well-informed by any expertise in security issues, and the Ombudsman therefore had not much recourse except to say that if the bank had checked everything and reported that everything appeared to be in order, he could not see that the customer could have a successful claim. So he was inclined, in other words, to rely on the banks' expertise instead of building up any independent expertise or putting the banks to any detailed proof. The last time I looked at this was a few years ago and things may have improved, so I cannot speak of the current position. I do think that it is necessary for the Ombudsman not merely to be honest, capable and independent, but actually to have some skills and resources available for testing the position when they are simply met with assertions that the bank's system has been fault-free and accordingly the fault must lie with the customer. At the moment, I fear that they are really no better than they were at resisting proof by assertion and it does not seem to me sufficient.

Q358 ***Earl of Erroll:*** This is directed at Mr Jones, the Information Commissioner's Office, and I want to restrict the answer just to banks because there are questions about it in the wider context. Surely under one of the data protection principles the banks are required to keep their customers' data secure, so you do have an interest in there other than the unsolicited aspect of emails, or whatever?
Mr Jones: Yes.

Q359 ***Earl of Erroll:*** Earlier you said you did not.
Mr Jones: Sorry. What I was trying to get at is the issue of fraud, and when we are talking about electronic communications that is under the Privacy and Electronic Communications Regulations and they really hinge on whether something is unsolicited, not whether it is unsolicited, and fraudulent, and deceptive and misleading. But you are perfectly right, under the Data Protection Act there is a clear principle in that Act that banks should keep the information secure and that is why, for example, we have initiated formal action in respect of the insecure disposal of customer documents without shredding. But it is the way the two bits of legislation fit together. I am sorry if I did not make that clear.

Q360 ***Baroness Hilton of Eggardon:*** If we can go on to actually buying things from shopping websites when one uses one's credit card. I have only dealt with amazon.com, but there is a whole range of them, is there not? What particular special risks do you see customers taking in that situation?
Mr Bohm: By and large, I do not think that using your credit card or revealing the credit card number, the expiry date and the security code on the back, which is about the full range of information you are required to reveal, is a risky thing to do. You do it all the time. You do it in a shop, on the telephone, and you do it on-line. People have been made to feel nervous about it, in my view, for no terribly convincing reason. If you ask people whether they think their bank account number is a confidential piece of information, I think many would say yes, but in fact it is on every cheque they write and hand to absolutely anybody, so it does not make a lot of sense to see it as a big secret. The same is true of the credit card. I think undue anxiety has been attached to the risk from the customer's point of view. I think the risk is greatest for the merchant, because in transactions where the customer is not present the merchant has no way of checking a signature against what is on a card or any other way of verifying. If the merchant claims the money from the bank and the customer rejects the claim saying, "I never dealt with this merchant," the bank will re-charge that amount to the merchant, claim it back through the credit card system, and will usually make an administrative charge as well. So merchants have no means of protecting themselves against that risk except on a volume basis. They have to hope that it does not happen so often as to render the acceptance of credit cards on-line uneconomic. There are systems deployed now under which the merchants should be able to get greater assurance from the banks, which are gradually being rolled out, but from the credit card user's point of view the risk seems to me to be extremely small.

Q361 ***Baroness Hilton of Eggardon:*** Does the same level of risk apply in Europe and the United States or would you see all the websites as being equally secure in that respect?

Mr Bohm: It is not that the websites are equally secure, it is that the disclosure of the information is fundamentally harmless to the consumer, and therefore I think it makes no difference where. It has to be said that if crooks light upon your credit card details to use fraudulently rather than somebody else's, you could be the one put to the trouble of rejecting the transactions. You are, to some extent, in the hands of the quality of your credit card issuer and if you have a low cost, cheap credit card issuer who does not care very much, you may struggle to persuade them and compel them to initiate a charge back and re-credit your account and any charges they have made. So you can be put to varying degrees of trouble when your credit card details are used for fraud. In the extreme case, if your credit card issuer refused to credit your account when you are entitled to have it credited you are left with initiating legal proceedings or resisting its legal proceedings against you to recover the money. That is not a happy position, so I am not saying it is a neutral effect, but the risks are exactly the same if you use your credit card in a shop which handles your information insecurely. So it is not particularly attributable to on-line use. We are all of us potentially liable to being impersonated by crooks and having some degree of trouble getting it accepted that it was not us, it was a crook. To some extent the fact that banks and financial institutions have taken up the practice of accepting electricity bills as capable of identifying people exposes them to the additional risk. Once upon a time, I do not think it would have occurred to them to do that so it is, funnily enough, the increased emphasis on identifying pieces of paper of this kind which are in fact rather easily forged or stolen which has actually exposed people to more risk, probably, than they used to be facing.

Q362 ***Lord Patel:*** I have a key related question, but in some US states there are laws relating to security breach notification laws where the businesses which lose personal data have to inform the individuals affected and maybe even widely inform the public. Should we not have such laws?

Mr Bohm: I am strongly in favour of extending breach notification and it is a principle which possibly has even wider benefits. There are two significant benefits to breach notification and they are different from each other. One is that the incentive on breach notifiers to avoid the breaches is increased, so it operates as a form of penalty, and that seems to me a desirable phenomenon. It increases the cost, the burden, the embarrassment. One hopes that it will therefore decrease the incidence, and that is distinctly desirable. It is a very effective way of doing it. It is self-policing largely. There is a second benefit, and that is to those whose data has been lost. They are better informed if they are later impersonated about how this might have come about. So somebody who says to his credit card issuer, for example, "I didn't do that transaction," and is faced with a recalcitrant issuer who says, "Well, how could that be?" he has a ready answer, "I was notified on this, that and the other date that my data was part of a batch which was lost by this or that institution." So it could very easily be, and that is particularly important in a case where, for example, there might have been a loss of data consisting of credit card personal identification numbers. So if somebody becomes aware that a cash machine has had a skimmer attached, in that case it is exceedingly valuable to all the customers whose cards have passed through that machine to know that there has been a compromise which might explain that fact that they have been defrauded, so that they have a response to a bank which says, "How could this be if you didn't do it?" So I think there are two distinct and considerable benefits and I would be strongly in favour of our taking that up, and indeed arguing that it ought to be extended across Europe.

Q363 ***Lord Patel:*** Have there been any prosecutions under the existing laws in the UK of merchants who has lost data because their computer has been hacked?

Mr Bohm: I am not aware of them. It is Mr Jones's territory as much as mine. I do not know whether he is.

Mr Jones: I am certainly not aware of any prosecutions and the important point to make is that, of itself, however serious that security breach was would not be a criminal offence, so they do not hold themselves open to prosecution at that stage. It would only occur under existing data protection legislation when they were already subject to a formal notice requiring them to take additional steps, but just to follow on from the previous point, we are certainly not opposed in principle to the idea of breach notification. We do think it is quite important that thought would have to be given to getting the thresholds right. We fully understand the name and shame element. Where I think we have some concerns is, what do you tell individuals they can do to mitigate the risk? If it is a very serious case where numbers have been lost, and I understand that what banks will traditionally do is actually withdraw those cards and re-issue. So we think there are some detailed points to address about what constitutes a significant enough security breach to inform the public and then what do you tell them that enables them to do something useful about it?

Q364 ***Lord Patel:*** So there is no offence even if a merchant has had his computers hacked and data is lost of a customer but he does not inform the customer?

Mr Jones: No, there is not, and the merchant does not commit an offence.

Q365 ***Lord Patel:*** As a Commissioner, do you have any powers through the Data Protection Act to act in response to breaches?
Mr Jones: As I say, what we do have is the power to issue a formal enforcement notice, which puts an organisation on notice to amend their practices. If they are actually in breach of the notice, at that stage it is a criminal offence but not before.

Q366 ***Earl of Erroll:*** If it is not hacking but an employee takes the data and sells it, does that make it a criminal offence?
Mr Jones: It may well make it a section 55 offence, but the interesting thing about that is that it is an offence which the data controller cannot himself commit. One of the employees can commit it by selling information, giving it to a friend, a colleague, and somebody can commit that offence by inveigling it out of the data controller, but however irresponsibly the data controller behaves he does not commit an offence.

Q367 ***Earl of Erroll:*** As this data should be kept in an encrypted form in the modern day and world on these databases, why do you not just pre-emptively issue your notifications to those companies which are not encrypting such sensitive data, and then you could act against them if they were in breach?
Mr Jones: Certainly we have not thought of that. I suspect it would be fairly hard to identify the large number of companies involved, but I think it is something which has not occurred to us.
Earl of Erroll: Pick some large ones.

Q368 ***Lord Harris of Haringey:*** Do we need special laws for e-crime, or is the current statute framework satisfactory? Perhaps you could also answer whether there are any gaps in the current statutory framework for e-crime?
Mr Bohm: I am not conscious of significant legal gaps. You may say that the one you have just identified and pointed to is a gap and you may say that the obligations of those who control sensitive information should be subject to more stringent controls, but if we look at the general field of crime and say, "Are things happening on-line which aren't crimes there but ought to be and would be elsewhere?" I think the answer is, "Not particularly." There was for a long time felt to be an inadequacy in the Computer Misuse Act, which has now been remedied. I think that there are problems in the field, but I would have said that they were problems which go more to the effectiveness of criminal investigation, sometimes perhaps the effectiveness of judicial understanding of the issues, and to trial and process management. So it is always easy to say more resources would be helpful, but ensuring that the police have the intellectual infrastructure to deal with crimes involving electronics and computers, and that the courts can readily grasp what they are about will, I suspect, do more to put wrongs right than tinkering with the legal framework at its base.
Professor Walden: I think there are two separate situations. One, does the existing criminal code cope with crime in cyberspace? The answer to that is, generally yes, but examples are found where that is not the case. The Fraud Act 2006 in part addressed a problem in an Internet environment, the fact that you could not deceive a machine, and therefore giving credit card details to a website and obtaining a service dishonestly was not considered to be a criminal offence of fraud until the recent amendments to the fraud rules. Likewise, in the area of child abuse images we have required amendments to existing law to cope with the new technology. On the other hand, you do have new activity such as denial of service attacks, where existing legislation requires supplementation, and that is what the Computer Misuse Act attempted to do and the latest reform is designed to address flaws or lacunae which have been identified in that computer specific context.

Q369 ***Lord Harris of Haringey:*** So essentially you are all saying, "It's absolutely fine and dandy. We don't need new laws to deal with e-crime because it's just a new manifestation of that"? I think in fact the SCL evidence talks about it being "a modern tool for those intent on committing established offences," but the consequence of that is that there is no data or no reliable data on the incidence of e-crime, there are no policing targets and actually there are few incentives, as a consequence, for the police to pursue this and to build up their capacity to combat it. Can I ask whether there are, in your view, any legal options short of creating a whole new category of e-crime which would enable us to distinguish between e-crime, say fraud using the Internet or similar offences which use more traditional means? Would there be a way of differentiating it short of creating a whole new category of offences?
Professor Walden: Currently the way crime is recorded in the UK does create a problem for fraud in particular. I think it would be fair to say that the vast majority of fraud committed today involves computers because the vast majority is accounting data, and data which gives rise to financial gains and loss is processed by computers. So I do not think, in that respect, there is necessarily need to distinguish where the tool differs from being a computer or being some other particular technique. Clearly, the question of reporting was addressed by the previous question in part because if businesses were required to notify of a breach that would, perhaps, incentivise.

We would get better crime reporting. One of the problems we have today is that at a commercial level the criminal justice system does not serve businesses well and they have no incentive to report certainly medium-scale fraud committed against them. From an individual perspective it is very difficult for consumers to know who to report to. If I suffer a fraud on Amazon and I went to my local police station, I think they would be quite nonplussed as to what to do.

Mr Bohm: I think you would create a difficulty in any case if what is already criminal is made criminal a second time in a new way, because you have got no way of knowing that prosecutors will charge it in the electronic form rather than the other if it is the same crime either way, so you will not necessarily improve the statistics. It is essentially an administrative problem, can the operations of the police be organised so that they discriminate effectively, and it is probably not helpfully addressed by creating a new layer of crime which they may or may not know how to use in the way you are hoping they would.

Q370 ***Earl of Erroll:*** So is the problem actually a lack of training and resource in the Police Force, so that the moment it appears to have an electronic or Internet facet to it they do not feel that they have the capability to pursue it or track down the offenders and prosecute them?

Professor Walden: I think it is in part a question of resource, but it is also in part a question of scale. The Internet allows the volume of crime, industrial crime, which we have not seen in a traditional environment and that in itself creates an insoluble resource problem. However much more money we put into the police, the fact that Operation Ore showed that we can suddenly have 7,000 potential suspects landing on the doorstep of the police is a difficult one to solve.

Q371 ***Earl of Erroll:*** But surely the problem, if you take what people have referred to, the Amazon or the eBay fraud, is that they are frauds where someone is either selling stolen goods or someone is paying for some goods and then getting some cash back off the person, without going into the detail of it? Those are frauds being perpetrated by people inside Britain, identifiable, pursuable, and they are probably doing it frequently enough to get quite large sums of money, so they would be worth pursuing. Any one incident may be trivial, but the person behind it is not trivial and if a burglar commits more than one burglary, we still pursue them and try to lock them up even if each burglary has been small.

Professor Walden: In part that is a question of the structure of the current Police Force in the United Kingdom. We have the local Police Forces in the 43 areas and then we have some national agencies such as the Serious and Organised Crime Agency. With these inter-regional crimes which may occur, perhaps, across the south of England, I think it has been well documented that this is a gap currently in our policing structure and the disappearance of the National High-Tech Crime Unit has led to the perception that that level two regional crime may not be properly served. There is an article in *The Independent* today from the Metropolitan Police Service calling for a new way of addressing e-crime at a regional level.

Q372 ***Chairman:*** Do you see this as an important issue? The very fact that you cannot distinguish these crimes from other crimes leaves us without targets for the police or reliable data.

Professor Walden: I think we do have a problem with data collection, but I think we have to recognise there are things we can know and things we cannot know. I think we need to establish reporting structures which are somewhat separate from the law enforcement agencies, and we see that emerging. We are seeing the establishment of an identity theft reporting mechanism. Within the area of child abuse images the Internet Watch Foundation provides a reporting mechanism. I think those sorts of bodies, which are independent from the police, will hopefully generate better statistics than can be expected from a traditional mechanism through the reporting to your local policeman about things which you have suffered, because evidence showed that in most cases if you suffer a virus you will go to your local PC World and tell them, as you are trying to get it mended, that you have suffered such a problem.

Q373 ***Lord Harris of Haringey:*** Can I just pursue this a little, because we heard evidence quite separately about bullying through the Internet and the fact that what distinguished it was the fact that this was within people's own homes and that it therefore was different in nature from traditional forms of bullying between children. Essentially this is fraud committed, if you like, in the privacy of people's own homes because it is being conducted over the Internet. Does that not place it in a different category in terms of the way in which it impacts upon people? We draw a distinction between a theft which is committed following somebody breaking and entering premises and theft which takes place in the open. Is there not an argument for distinguishing between fraud or theft which takes place through the Internet because of that personalised nature of the crime?

Professor Walden: Yes, I think that argument can be made. The way in which we record statistics is different, clearly, from the way in which we categorise crime and I do not think we would benefit by proliferating new types of offences designed to capture traditional crimes committed within a new environment. There certainly may be, and probably

would be, a policy benefit from recording the fact that these crimes are committed in different ways, but I do not think it requires new offences, it just requires new reporting mechanisms.

Q374 ***Lord Harris of Haringey:*** But the nature of the offence is not different because it is committed in a way which people regard as personal, as part of their private world, part of something where they like to think they are secure because it is in their own home?
Professor Walden: I personally think not.

Q375 ***Baroness Sharp of Guildford:*** Moving from reporting to pursuing criminal charges, in the memorandum from the Society for Computers and Law you claimed that there may be a reluctance within the Crown Prosecution Service to pursue criminal charges where the only charges available are those under the Computer Misuse Act 1990 or the Data Protection Act 1998 for computer-related crime. What sort of evidence have you got to support this and what types of offence are most affected?
Professor Walden: I think part of the problem is that historically the offences did not necessarily attract a particularly high tariff so that, for example, the offence of unauthorised access gave rise to a maximum penalty of six months' imprisonment. In terms of evidence, I have been involved for the past five years in training Crown Prosecution Service personnel to specialise in high-tech crime prosecutions, so the evidence which I put to the SCL and which was incorporated in this paper was from that trainee exercise where we have trained over 150 CPS prosecutors in high-tech crime. The constant feedback was, "Well, there's uncertainty about the application of the law in the area of computer misuse, the history of the Act.. We've had continual bad judgments, bad case law, which may have been corrected but we have problems in explaining the technology to jurors and explaining the technology to judges." In the majority of circumstances we are talking about a computer being used as a tool to commit a traditional offence, so let us use the traditional offence and ignore the legislation which really addresses the tool, which is the Computer Misuse Act.

Q376 ***Baroness Sharp of Guildford:*** The evidence you have got from this really stems very largely from your work training with the CPS?
Professor Walden: With the Crown Prosecution Service, yes. It is a concern that prosecuting under the Computer Misuse Act is more likely to give rise to problems than using traditional offences.

Q377 ***Lord Sutherland of Houndwood:*** This is a question for the Information Commission but it starts with evidence from SCL in fact, who have told us that they are not aware that there has been any enforcement by the Information Commissioner, whether at the request of Ofcom or anyone else, of Internet providers taking appropriate action under the specified regulations. I do not know whether they are simply not fully informed, whether there have been enforcements, but what are your comments on this?
Mr Jones: No, they are perfectly well-informed. There has not been any such action. What I would stress here is that the way the Privacy and Electronic Communications Regulations work is heavily towards people reporting things to us which appear to be breaches and then asking us whether we will take action. The reality is that the action we have taken over these regulations has reflected those areas which we have had large numbers of complaints about, and they have actually been to do with telesales and faxes, not so much with emails and not to my knowledge much at all relating to ISP security.

Q378 ***Lord Sutherland of Houndwood:*** Is this because you are not being notified or not being made aware of such offences, or because they are not considered to be important?
Mr Jones: No, it is not that we would not consider them important if we had evidence of them. What I am saying is that we have not had evidence of them. I entirely accept that that does not mean to say that there are not weaknesses there, I am just saying that they have not been drawn to our attention.

Q379 ***Lord Sutherland of Houndwood:*** SCL imply that they are not completely satisfied with this and they would like to see Ofcom involved in the enforcement of regulations. There is a question of whether they have the powers to do so, but if they were to be involved would there be advantages, disadvantages, if I could ask both of you that?
Mr Jones: The way the mechanism is set up at the moment is that because of the way Ofcom works and because it has a wider staffing than we do and has a technical expertise in certain areas that we do not, if it brings to our attention what it sees as significant failings then we can actually take enforcement action on the basis of that. We are perfectly happy to do so, it is just that it has not happened yet.
Professor Walden: I think the idea put by SCL is that essentially Ofcom is the better resourced and more experienced regulator in respect of the industry and therefore, in part to help the Information Commissioner's Office, Ofcom will be well-placed to address these issues.

Q380 ***Lord Sutherland of Houndwood:*** But presumably they are in a position at the moment to draw the attention of the Commissioner's Office to

such but they have not done so, so it would not be much of a step forward, would it?
Professor Walden: Ofcom does not have a very clear remit in the area. It has many other things to do. Were it to be given a specific remit in this area, then I think it would obviously have to devote resource and manpower to tackling that topic.

Q381 ***Lord Sutherland of Houndwood:*** Is that wishful thinking, or do you have evidence that that is how it would move?
Professor Walden: Ofcom does have responsibility in respect of persistent misuse of networks, for example, under the Communications Act 2003 and within the scope of that were changes to be made to expand that remit somewhat then I would imagine Ofcom would take that responsibility. It has taken action against those who persistently misuse their electronic network.

Q382 ***Lord Sutherland of Houndwood:*** Would it need additional powers to be able to enforce?
Professor Walden: I do not believe it would. I think the existing legislation would be sufficient.
Mr Jones: I agree, yes.

Q383 ***Lord Young of Graffham:*** This is really for Professor Walden. In the Society's submission to us you are proposing that ISPs should be legally required to put minimum standards of technical protection measures in place, in other words protecting the centre rather than the end to end protecting in our machines. What sort of filtering or blocking do you really think would be appropriate?
Professor Walden: At this point I would say that we are not actually saying the security measures need to be necessarily at the level of the ISP. We do not suggest that filtering or blocking at the level of the ISP is the solution, we are just saying that the ISP has a very good, close relationship with the user and therefore it seems an appropriate point of control. What I mean by that is the ISP can encourage and help the user to implement controls at the user's end. So it could be offering filtering and blocking software and the necessary training and implementation of that blocking software at the end user point, but it is the ISP who is in a good position to facilitate that implementation.

Q384 ***Lord Young of Graffham:*** But you do point out in your submission that if you have an unprotected ISP, one which does not put anything in the centre, and I as a user do not take any precautions, not only can my machine be infected but I can start to infect other people on the network?
Professor Walden: Yes. We say in the submission we could leave this completely to the free market and people could choose whether to go for the high grade, perhaps slightly higher cost, fully secured network or go for a bare Internet provision or access. In the area of security it is well known that obviously in network security you are only as secure as every node within the network and therefore if we do not consider the obligations of the end users and any obligations of ISPs we are potentially exposing ourselves.

Q385 ***Lord Young of Graffham:*** I am a great advocate of the free market, but even I do not think that road crossings should be unregulated. I am quite prepared to put up with traffic lights, for example. What slightly concerns me is the ability of one careless user to infect many others. Do you not think there is a role for the centre, the ISP itself, to put in standards?
Professor Walden: Yes. I think there is. I think there are concerns about their capabilities to do that. One of the recent debates is in respect of child abuse images and the Government's announcement last year that it is going to require all broadband access providers to filter child abuse images on the basis of a list promulgated by the Internet Watch Foundation.

Q386 ***Lord Young of Graffham:*** Is there not a difference between regulating content and actually regulating viruses of any sort or other? Once you get into content you will be getting into very, very dangerous ground?
Professor Walden: I think you are getting into very dangerous ground, although viruses are just a form of content, and whereas an ISP may filter for viruses, then there is the question of should they filter for unsolicited communications, spam, and should they filter for child abuse images? There is a slippery slope where once they get asked to filter and block for one thing they will be asked to filter and block for others. That is why I must put on record that the SCL does not suggest, and has not in its submissions, that filtering and blocking be implemented at an ISP level. What our submissions suggest is that the ISP must bear some responsibility and is a good partner with end users to improve the security measures which take place both at an end-user level and at an access level.

Q387 ***Lord Sutherland of Houndwood:*** It may not be an apt comparison, but your Society is very happy to tolerate regulations about the sale of guns and alcohol and there is not a slippery slope that automatically follows from that. I would have thought viruses are in a different category from straightforward content.
Professor Walden: I am Vice-Chairman of the Internet Watch Foundation and I am aware that the organisation does receive suicide websites, extreme pornography, which the Government is going to legislate on, and religious hatred, which it legislated

on last year. We are seeing a growing concern about the content which is available over the Internet and that is where our concern lies. If you think there is a solution in blocking and filtering at an Internet Service Provider level, that could, by fair means or foul, be extended to a range of content which I think will fundamentally damage the Internet as an environment for the free exchange of information.

Q388 ***Lord Sutherland of Houndwood:*** Could or would automatically?
Professor Walden: Could.

Q389 ***Lord Young of Graffham:*** It would allow you to filter politically, for instance?
Professor Walden: Exactly.
Lord Sutherland of Houndwood: I understand that, but in the same way the gun law was changed as a result of what happened in Dunblane, now, whether rightly or wrongly, most people accept that some sort of law is appropriate there in a way which is not appropriate for motorbikes and motorcars.

Q390 ***Lord Young of Graffham:*** I am just wondering whether you could not legally distinguish between malware of any sort and viruses, whatever, and content, because I think one is quite clear. It is a virus which sets out to do harm one way or the other and the other is an expression of opinion, however distasteful you may find it. I would be very concerned if we started to get into free speech. There are some boundaries there, but I am also equally concerned that if the Internet is to flourish we have got to be able to be within a reasonably protected environment. I think when one careless user can start infecting other people we just have to be very careful, that is all, and I just wondered whether you were aware of any other technology or reason why the ISP could not be expected to actually put traffic lights into the centre of the network?
Professor Walden: Yes. I think the nature of the Internet as a network of networks, the nature of the technology which underpins it, again taking child abuse images as an example, whereas we have seen a great growth in the availability of child abuse images via the Worldwide Web, we are now seeing that that is being replaced by the exchange of such images using peer to peer networking applications, which essentially would bypass blocking exercised at an ISP level. Therefore, people's ability to use this technology currently outstrips our ability to impose controls and we could focus all our attention on imposing obligations on the ISP and miss the target.

Q391 ***Lord Young of Graffham:*** That is why I am not concerned with the content. I am looking at phishing and I am looking at the other ways in which people cause harm.
Professor Walden: Yes. It is all data. It is all zeros and ones which go across the network, whether it is a virus, a child abuse image or a political statement. Our ability to distinguish at a network level the stream of data which is passing is difficult without perhaps capturing too much legitimate data or not capturing the illegitimate data.

Q392 ***Chairman:*** Would you like to say a little more about that? How easy is it to distinguish a pornographic image from any other image?
Professor Walden: The technology does exist. I do not know in terms of its percentage of reliability, but you are going to have a whole problem with false positives whereby, for example, one of the classic examples is that talking about Middlesex is going to cause problems with certain filters because the county ends in the word "sex".

Q393 ***Chairman:*** I am concerned about images particularly, because this is something which has worried me for a long time. Ultimately, presumably somebody has to look at these images, do they?
Professor Walden: The technology is certainly sophisticated enough, as far as I am aware, to distinguish image data and flesh tones within a particular message. I do not know the technological developments to extend it so that you can avoid such filtering software, but I am sure the clever people out there are making sure there are ways to get around such software.
Lord Young of Graffham: I have a few years' experience of looking at red eye in photographs and there are enough false positives in that, and that is a very small thing. Pornography is in the eye of the beholder and it is a value judgment more than anything else, and that becomes extremely difficult, I would have thought.

Q394 ***Earl of Erroll:*** What is your view of the idea that software manufacturers should be held liable for how well their software works, and particularly for security flaws in their software, rather than relying on the disclaimers and statements that it is up to the customer to decide whether it is fit for purpose?
Mr Bohm: I wonder if I might respond on that one? I think there is a good deal of agreement that there is an incentives problem with insecurities in software, namely that the suppliers and the creators by and large do not suffer the adverse consequences to the same extent as their customers and therefore do not have adequate incentives to eliminate the flaws. I think the next step in this argument has not been as well explored as the first proposition. I very much agree with that proposition. I do not think things are entirely satisfactory in terms of incentives. I think that too much defective software has got out. The question of just exactly what you do, having reached

that conclusion, is, not surprisingly, quite difficult. You can imagine an extreme approach, the motor vehicle approach, in which there is a set of construction and use regulations with which all software must comply before it is fit to be used on the Internet, and you have got to take your computer in for an MOT test and you have got to take a driving licence and get yourself re-licensed. A regime of that kind I am only setting up as a straw man, because it seems to me grossly disproportionate to the type of loss and injury caused by the defects we are talking about as compared with what motor vehicles do. Secondly, and possibly a more interesting drawback, is the fact that the speed of response of such a system of that kind to new developments and changes would be hopelessly slow. If you think of some of the zero day exploits in which a patch is released (or, as Microsoft like to call it, an update) and people disassemble it, work out what the problem was that it is trying to fix within a few hours and attack the computers of those who have not yet applied it, and you imagine a regulatory system attempting to keep pace in that environment, you will see why I do not think it is feasible, even if it were proportionate, which it probably is not anyway. So if you step away from regulation as a way of dealing with the incentive failure, you tend to fall back on saying, "Well, let's make them legally liable to their customers," or in an English law context, "Let's stop them contracting out of those liabilities," and to some extent we do hint at that because exemption clauses do face reasonableness tests, and so on, and we have tended to take that approach. Will it do enough good? I suggest that it will not do a lot of good for a number of different and independent reasons. One of them is that the people who suffer the loss are a long way down the chain. Somebody gets hit with a denial of service attack because out on the Internet 10,000 computers have had a weakness exploited but their owners do not realise they are being used in a concerted attack because somewhere out there there are crooks taking advantage of a weakness. The person injured is many, many steps down a chain—and there is certainly no contractual connection with a software supplier—in which third party actions intervene to cause it, and hoping that you can somehow incentivise the manufacturer to have eliminated those defects by enabling someone to sue is not very likely in that context because the people who have got the real incentive to sue are simply too far down the chain. The legal difficulties are almost certainly too great. Our attempts to stop people contracting out of unfair contract terms may not work very well because a lot of software is the subject of international supply contracts, to which those laws tend to either not apply or apply differently and are governed by foreign laws. So the legal mechanisms are not terribly good. The people who do have a position to sue are the customers who can sue PC World, but each of them suffers probably trivial losses and they are simply not going to take up their rights. They are not going to risk getting a costs award against them if they sue for tuppence ha'penny anyway. In other words, the risks and losses are diffused by the Internet and it is not an environment in which beefing up direct liability is an easy thing to do. It is very difficult to get it targeted right. If you get draconian with all the people who supply any software to anybody anywhere, you will impose terrible penalties on all sorts of small tinkerers in the open source community, who will be discouraged from contributing. So you will be reproached for stifling innovation and helping to lock in the monopoly position of large suppliers. I think it is an area fraught with difficulties. The one thing which I think you can do, and I think it harks back to earlier questions today, is defect notification, rather like breach notification. Defect notification is not particularly onerous. Everybody who does supply software on a commercial scale could be obliged to set up defect reporting procedures, into which all users can easily contract, so that if you acquire a bit of software the web page through which you acquire it has a button to tick which says, "Warn me of defects," and if those who then supply it are obliged to notify the defects promptly you do have something reasonably workable, reasonably consistent with what best practice requires at the moment, arguably, and reasonably useful for customers. You are also applying a significant incentive. The more reputation-based people's businesses are, the more significant it will be to compel them to own up to errors and defects and to provide remedies. So I think there are some pressures which could be applied, but I am cautious in this field because there are so many things you can try and make people do that would work badly and work adversely, but I think it is a field to move cautiously in even if you 100% accept, as I do, that the incentives are not entirely happy in their operation as they are.

Q395 ***Earl of Erroll:*** I imagine the first part of your reply people use against the Sale of Goods Act and goods having to be suitable for the purpose for which they were intended, but I will not get drawn into that discussion! I know that the SCL suggested that perhaps software could be labelled with traffic lights to suggest how good it was for purpose. The trouble with that, presumably, is who does the testing, who does the certification, how do you make sure that it is all up to date and how do you deal with bugs after it is released?

Professor Walden: Yes. I think the model we were thinking of is all telecommunications equipment has to be type approved. That type of approval process is essentially a self-certification process whereby

manufacturers of Nokia, for example, do not have to submit their telephone to a third party for certification as meeting minimum standards, and those minimum standards include that it will not kill the user, it will not kill the network, it will not do those things. I think a self-certification scheme would be perfectly feasible. Clearly, the question of who sets the standards is a complex issue, but again industry would seem best placed to start down that road.

Q396 ***Earl of Erroll:*** Yes. I tend to look at reviews, I must say, in magazines. What about what is almost a sell by date? We have been looking at ideas of whether software might be labelled to make sure it is sufficiently up to date when it is being sold. Do you see any legal problems with this requiring shops to report this when they are selling something to customers as to whether the software on it is sufficiently up to date or not?
Professor Walden: I do not know if there are statistics in terms of how much software is now sold in shops as opposed to sold on-line.

Q397 ***Earl of Erroll:*** Or on-line then?
Professor Walden: Again, the idea goes back to an earlier question. In the UK certainly we do not generally criminalise negligence and if we do not criminalise it, if it just gives rise to some civil liability, the ability of individuals to take legal action under the English legal system is so expensive I am not sure it necessarily offers some benefit unless we can look to a regulator who acts as our surrogate. The Information Commission is not in that position. Ofcom could be in that position in certain circumstances in respect of those who provide Internet access. In the software industry there is no obvious party which would necessarily be well-placed to take action on our behalf.

Q398 ***Earl of Erroll:*** Trading Standards can make sure the shops are selling stuff which is up to date and that you are not buying out of date stuff which is going to immediately leave your machine open to viruses when you buy a new laptop or something?
Professor Walden: Sure. Were it to be for industry to set standards about when software is in date or out of date, then that would be a potential mechanism.

Q399 ***Lord Young of Graffham:*** Could we not set standards so that when the first piece of software is used and accessed to the Internet it downloads any upgrades? In other words, make that automatic, because that would cover that point. So, in other words, however old the software was, once it was being used it would be upgraded?
Professor Walden: Yes. I think the complexity of software and the complexity of how people use that software would potentially cause some problem with that system, but yes. With Microsoft Windows, for example, they have improved the way in which those updates are distributed and installed on people's machines.
Lord Young of Graffham: It drives you mad because it happens every Tuesday!
Chairman: Most software companies are doing that now, but it might be made a requirement. Let us move on because we want to have a chance to talk to you about spam.

Q400 ***Baroness Sharp of Guildford:*** Do you think that the current UK anti-spam laws are adequate, and if not what should we do to improve them?
Professor Walden: From a criminal perspective, which is an area I have been concerned with of late, some jurisdictions have criminalised not the sending of spam but actions related to spamming activities, but I think English law is currently sufficient. The Computer Misuse Act would be the most relevant legislation in most circumstances and I do not think the sending of spam *per se* is necessarily an area for criminal law, and I think the Data Protection Act and associated legislation is more suitable.
Mr Jones: Just two quick points there. First of all, when you look at the way the Privacy and Electronic Communications Regulations apply to unsolicited emails, rather strangely they do not apply to unsolicited emails sent to a corporate subscriber, that is to a company or an organisation. That is slightly strange because the rules applying to phone calls and to faxes do apply to corporate subscribers. So first of all there is actually a mismatch between what people would traditionally think of as spam, the bulk sending, the indiscriminateness, but the way these regulations apply it distinguishes between the recipient, regardless of the content of the message. That is something which is within the DTI's purview. It does seem slightly odd. They did change the rules fairly recently relating to phone calls, so that would be a possibility.

Q401 ***Baroness Sharp of Guildford:*** Does that explain why I get so much more spam and phishing on my parliamentary email than I do on my NTL one at home?
Mr Jones: It may well do. It might be because it is also very easy to work out what parliamentary email addresses are. I think they follow a standard format. The other thing which is true is that because the rules are part of the package which applies to phone calls and faxes, the current rules treat them the same in terms of penalty. I am not saying it is impossible, but I think there would be some difficulty in deciding that one form of communication, regardless of its content, was inherently more heinous than another. So I think that would be quite a difficult balance to

get right if you were to think of changing the law there.

Q402 ***Baroness Sharp of Guildford:*** How many people in the UK actually send spam, and have there been any prosecutions at all?
Mr Jones: We have not prosecuted anybody, for two reasons. First of all, we still get far fewer complaints about email than we do about phone calls and faxes, so the action we have taken thus far has been against serial abusers of the fax rules and the phone rules. That is the first point. The second point is that, as I said before, they would only commit an offence when they were subject to an enforcement notice and ignored it. The email complaints that we get at the moment, some of them are not valid because they are actually received by a corporate subscriber, and that I have already explained. Some of them are perfectly legitimate, where a UK company just sort of got things wrong, it had made a mistake, and that is fairly easily put right, but there are some from overseas and others which are good at hiding themselves. But as I say, at the moment the numbers of complaints we receive are much smaller than phone calls.

Q403 ***Baroness Sharp of Guildford:*** I believe a lot of spam emanates from Eastern Europe, and so forth. Is much effort put into identifying the senders of spam?
Professor Walden: Internet service providers have an incentive to try and address this issue, and again I think in terms of effective law enforcement we do need to look at Internet service providers working in co-operation with each other on an international basis to try and stop this sort of activity. I think the activity which we have seen to date has probably been most effective in that area.

Q404 ***Baroness Sharp of Guildford:*** What about lottery spam and the advance fee fraud scheme? How much investigation is there of these and how much money is being recovered? Have you any idea?
Professor Walden: I understand from a recent visit to the Serious and Organised Crime Agency that Nigerian 419 fraud has been one of their major areas of activity over recent years. Successfully? I do not have any information about.
Baroness Sharp of Guildford: No. Thank you very much.
Chairman: We are really running out of time, but if we can quickly just take the last question.

Q405 ***Lord Harris of Haringey:*** In the USA many prosecutions of spammers have been undertaken as third party actions by AOL, Microsoft, or whatever. Is that possible in the UK, and what would be the arguments for and against doing so, going down that road?
Professor Walden: With private prosecutions the general default rule under English criminal law is that private prosecutions are perfectly possible. Some legislation actually requires that the Information Commissioner or other regulatory authorities, or the DPP has to lead private prosecutions, but it would be possible under UK law.

Q406 ***Lord Harris of Haringey:*** None of the legislation here, in terms that it might be used against spammers, has that requirement, that it has to be led by the Information Commissioner or that the Attorney-General has to personally sign it off, or anything?
Professor Walden: I do not believe so. The DPP has the right to take over a private prosecution which has been commenced. For example, under the Computer Misuse Act I could bring a private prosecution.
Mr Bohm: Some action taken, I think by private parties in America, may have been civil rather than criminal and may have relied on the fact that in the United States class actions are sustainable on a much more simple basis than they seem to be in the UK. I am not a litigation expert, but it does seem that some organisations have succeeded in bringing proceedings representing large numbers of those who have suffered. I think the difficulty where that is not possible is that each individual person who receives spam suffers a pretty small detriment and is not really likely to take action of a burdensome kind to pursue it beyond making a complaint, possibly, whereas if the rules about class actions or representative actions were easier and if the costs rules were different so that you did not have to pay costs when you lost, and indeed if you could recover something substantial when you won, then you might see a litigation solution to the problem. I did want to draw to the Sub-Committee's attention one aspect of spam which is not, I think, always given the attention it deserves, which is one of the consequences. With my volumes of spam I get statistics from my scanning service and I am getting about 40,000 a day at the moment, of which happily I do not see very many, but the result is that in order to trim that down to tolerable proportions—and it is rising steadily, a few months ago it was 20,000—the scanning or filtering which takes place necessarily risks false positives and although I am offered the false positives they can get that wrong. Email is therefore increasingly unreliable as a means of being sure that you have received a communication. It is a side-effect of spam and it is, funnily enough, a side-effect with potential legislative consequences because as the courts become more modernised and willing to rely on email and as other official channels begin to rely on electronic communications, the public at the other end of these are at risk of being told they are deemed to have received something because an email was sent to their

last known email address three weeks before, and they simply have not succeeded in retrieving it from intolerable piles of filtered spam. So there is an awkward side-effect which points to a certain amount of need for caution as public services become more electronic. People's security is, in effect, affected because they are deemed to have received communications they have not received.

Q407 ***Chairman:*** That opens up the question of how many filtering systems notify the sender that their message has been filtered out and not delivered.
Mr Bohm: It assumes, of course, that the senders' systems are capable of noticing responses. Many people send messages, official bodies send messages out saying, "Do not reply. Your reply will not receive attention." Of course, if that bounces, the bounce will not receive attention. So it raises a quite complex delicate question about how these things ought to be done, and indeed where the risk ought to lie, but it is fairly dangerous for the individual to in effect be willing to be bound by emails addressed to them nowadays, given the environment we have.
Lord Harris of Haringey: That raises quite important problems which we may want to follow up..
Chairman: I think we should pursue this, yes. We have run out of time, Professor Walden and Mr Bohm. Thank you very much indeed. It has been a very useful session to us and if anything occurs to you that you think we should know, please write to us. Thank you very much.

Examination of Witnesses

Witnesses: Mr Mike Haley, Deputy Director for Consumer Advice and Trading Standards, Head of Scambusters Team, Office of Fair Trading, and Mr Phil Jones, Assistant Commissioner, Information Commissioner's Office, examined.

Q408 ***Chairman:*** Mr Haley, thank you very much for joining us. I think you have been attending the session so you know how we proceed. Would you like, please, to introduce yourself and to make any opening statement, if you so wish?
Mr Haley: Thank you. My name is Mike Haley and I am the Deputy Director for Consumer Advice and Trading Standards at the Office of Fair Trading and one of the teams I head is our national Scambusters team which deals with mass marketing scams. It is probably better described as mass direct marketing scams, including those scams disseminated by email and on the Internet. Perhaps I will touch on why we define scams and fraud as different problems for consumers a bit later. I do want to speak a little bit about the OFT's role, because I think it is slightly different from some of the other contributors, who have a direct interest in security and fraud, in that we are the lead competition and consumer protection agency and our role is about making markets work well for consumers.

Q409 ***Chairman:*** That was part of the answer to my first question, which is what is OFT's role with regard to personal Internet security?
Mr Haley: We see the Internet as providing an unrivalled potential for cross-border transactions, in particular opening up a whole new world for consumers to shop on-line. We think this drives competition across the internal and global marketplaces. We are currently undertaking a major market study, a market study is an in-depth survey of the Internet as a shopping channel and that will produce recommendations for actions. We plan to publish that report in the spring of this year. It is a wide-ranging study which will be largely descriptive, covering a wide range of issues, including the regulatory framework around Internet shopping, consumer awareness of rights, business compliance with regulations and enforcement of consumer protection laws in the on-line environment, and also looking at the barriers there may be for consumers and business to take full advantage of the Internet as a shopping channel, that is why we have an interest in the issue of consumer confidence. There are a number of factors we are looking at which may affect consumers' confidence about participating in on-line markets and one of those factors is personal Internet security. Although it is only one, others will be addressed, such as the failure to deliver products and services, but it is the sphere of consumer confidence which gives us a real interest in personal Internet security. We are considering whether there are real threats and what are the perceived threats, and whether they are becoming a barrier to the continued growth of the Internet as a shopping medium, because we think that consumer confidence for on-line shopping is probably quite fragile because of a number of factors, including the amount of spam, the amount of viruses and other factors which you have been touching upon today.

Q410 ***Chairman:*** Can you describe the London Action Plan and what is OFT's role?
Mr Haley: Yes. The London Action Plan is basically a simple work plan promoting flexible action-orientated spam enforcement. I think it differs to other international arrangements. Its particular role is looking at how to facilitate enforcement action against spammers through public and private

agencies and through the different agencies which have some interest in spam. It has members from about 27 different countries now, about 80 members, and they include government agencies, whether they be data protection agencies, telecommunication agencies, consumer protection agencies, Internet Service Providers or security companies. It works through a number of mechanisms of networking. We have regular conference calls where the members will call in and share best practice, talk about enforcement cases which are ongoing, information they may wish to share, and in fact there is one of those regular conference calls tomorrow if any of the Committee members would like to attend and listen in. That is the primary mechanism of how it works, information exchange. We also hold a conference once a year. For the last two years the conference has been in collaboration with the Contact Network Spam Authorities, which is an EU network of spam authorities in Europe. We also have regular emails because people get to know each other and their interests, and then there are bilaterals which then look at particular spammers to take enforcement cases. So it works in a loose and flexible way, trying to reduce the bureaucratic barriers to the minimum in terms of membership, particularly across the public/private divide.

Q411 ***Chairman:*** How effective is international co-operation currently in dealing with spam?
Mr Haley: It is quite good where there are enforcers who have a specific duty to enforce spam and have competent technical investigative staff and who have a real drive to go after spammers. An example would be OPTA, which is the independent telecoms agency in Holland, which is a member of the London Action Plan, it has a small dedicated force looking at spam and they are very competent officials. They have given training to some of my staff and internationally. They have recently contacted the Australian Communications Agency (ACMA), which is part of the London Action Plan, to look at a spammer from Australia targeting Holland and collaborating to track down the spammer. So I think it is effective in that way. It has also been effective in opening up the organisations for those developing countries and countries from which the threat originates, such as Russia, India, China, to be members of this network, who may have taken a lot longer to become a member of a formal network because of political problems, perhaps, but people like the Union Network of Beijing are members of the London Action Plan and that facilitates good contacts whereas before we may have given up, thinking, "They're from the Ukraine, or from China," and you may be aware that a lot of our spam investigations just would have finished in the past.

Q412 ***Chairman:*** What percentage of this work is effective? In the Dutch/Australian case did they catch the spammers and prosecute them in Australia?
Mr Haley: The Dutch have been particularly effective and they quote figures where they have reduced spam from Dutch spammers to Dutch citizens by 70%, which is a very impressive figure.

Q413 ***Chairman:*** They have done this by actually prosecuting people?
Mr Haley: Prosecuting and other disruptive measures, working with Internet Service Providers, but I would not want to give a false impression that in Holland you will not get spam because obviously so much spam originates from other countries around the world, but in terms of cleaning up their own backyard they have done, I would say, a particularly effective job.

Q414 ***Chairman:*** A much better job than we have done?
Mr Haley: I think in the UK—and I would back Phil here—we have very few complaints about UK originating spammers, that is spammers who are not sending spam to corporate addresses, and I think some of the spammers in the UK—and there are some—have been quite cute in recognising the differences in the rules and not spamming, perhaps, to my personal address but spamming me at my OFT address and therefore not being spam in terms of it being unsolicited.

Q415 ***Chairman:*** How easy is it to be a UK spammer and to be unidentifiable as a UK spammer?
Mr Haley: I think it is quite easy to identify someone to be a UK spammer. The problems we have faced in particular cases have been where it has been a spammer who is spamming from the UK into other countries, particularly outside the European Union, because it has been difficult, if not impossible, to act against someone who is not affecting the economic interests of the UK consumer. I think in an international global market if we cannot act to protect consumers in another country, we will end up with spammers targeting each others' countries with spammers sitting in third countries.

Q416 ***Chairman:*** Is the European Commission a party to the London Action Plan?
Mr Haley: Yes, the EU is.

Q417 ***Chairman:*** To what extent do you co-operate with the Commission in developing new proposals for European action or legislation on spam, or e-crime more generally?
Mr Haley: There is good co-operation with the European Union and with the OECD. The OECD have produced a spam toolkit. Myself and others

from the EU and other European countries around the world were members of the working party putting together the best practice for the spam toolkit. As I mentioned, the two conferences we have had with the London Action Plan, when they have been in Europe, have been with the Contact Network for Spam Authorities, so they have set up a network of spam authorities. I think within the European Union we have a common rule as well, so we know that with the Directive, where the privacy and electronic communication regulation has come from, we have a similar regulatory framework. I do not think we see many problems which are intra-Europe. Things were coming into Europe, from spammers from around the world into Europe and elsewhere.

Q418 ***Chairman:*** The European group is in Greece, is it not? Am I right?
Mr Haley: I think one of the last meetings was.

Q419 ***Earl of Erroll:*** Could I just ask a quick supplementary, which is that you have just highlighted an area where maybe a new law is required because the trouble is that a spammer can sit in the UK, spam abroad and is untouchable under UK law. Unless you manage to get an extradition together, nothing can be done about it. So is this just an example where the evidence we have just been given by the two previous witnesses is incorrect, in that here is somewhere were we should in fact have specific e-crime laws, because spam is really an e-crime?
Mr Haley: Whether or not a specific e-crime law is needed, I certainly agree that there is a gap. In fact I investigated a specific case of a spammer based in London targeting US consumers. It was just after 9/11 and he used a fake top-level domain name. So he emailed spam saying, "Why be dot US when you can be dot USA? Be patriotic," and this went out to millions of US consumers, and it was a fake. You could not use that Internet address, and he made several hundred thousand pounds. When the Federal Trade Commission from the US approached us we struggled to take any action because no UK consumers had been affected by the spamming operation. In the end there was a successful action which we took by getting undertakings from him not to do it again and the Americans tried to seize assets both in the US and with UK banks. It was a successful co-operation, but it exposed the gap that we could not take a court action to stop him spamming outside the European Union. I think we are not the only ones who have that problem because we have also had spam from the US into the UK with no US detriment.

Q420 ***Earl of Erroll:*** Therefore it is not extraditable?
Mr Haley: In this case, because our powers are only civil powers, it would not be a criminal offence. We only have civil injunctive powers for regulations 22 and 23 of the PCRs, plus our main role is actually looking at the deceptive and misleading nature of spam. Because we regulate advertising, we are not concerned with spam *per se*, we would leave that to the Information Commissioner if it was not deceptive or misleading, but when it is misleading like that spam was, we do see it as our duty to use the powers we have. But he could not be extradited because it was not a criminal offence which was being investigated.

Q421 ***Lord Patel:*** Can the London Action Plan be effective without any legal force?
Mr Haley: It is effective in a number of ways by establishing a network of contacts, but I would point out that it is on a "best efforts" basis. It does rely on the individual's commitment to co-operate. I have an example of where it has failed and we need further legal clarity, which was when OPTA, the Dutch agency, approached our agency under the London Action Plan to provide information about a spammer using a Yahoo.co.uk account. We have powers to gain information under section 224 of the Enterprise Act, but our legal adviser said we could not use it to gain information to pass on to the Dutch authority because they were not a Community enforcer under our consumer protection laws. So in that case there were again no UK victims of that spam and we could not use our powers to get the information and pass it on. So in that case they had one of the top 10 spammers and required information to stop them and we could not obtain the information to pass it on to them in a lawful way. Yahoo were quite right not to give that information over. I am not criticising Yahoo because there was not a legal gateway for them to give that information to us. We have also had a problem in the London Action Plan where Spamhaus, an organisation which is a kind of watchdog for spam, had given us information there was going to be a major spamming campaign over a weekend, and they gave us the information. When I contacted the relevant Internet Service Provider, who is a member of the London Action Plan, without a court order or any other further action they were not able to stop that spamming campaign. I think in the end they took a decision based on pressure to pull that campaign and stop it happening, but there was no legal requirement, it was just best efforts.

Q422 ***Lord Patel:*** So you feel that the UK spam laws are adequate?
Mr Haley: I think in those two instances of international co-operation there could be much improvement in ensuring that we have gateways to

share information with agencies which are spam enforcement agencies elsewhere, because we do not always have those gateways. Secondly, I believe it would be very helpful if we could take action against spammers in the UK who are targeting non-UK consumers, because there are two gaps in that area. That is my enforcement experience.

Q423 ***Lord Patel:*** Are there laws internationally beginning to converge relating to spam?
Mr Haley: No, there are not, because we have the two different models of opt in and opt out, choices for consumers. I think the Americans are very wedded to their model and the European Union has taken its decision that we should have a different model, so I do not see convergence along those lines at the moment. What we do see through organisations like the OECD and the London Action Plan is encouraging those countries which do not have spam laws to bring in spam laws as recommended under the spam toolkit which the OECD produced, which has model laws.

Q424 ***Lord Patel:*** Does that not make it difficult to prosecute if there are different laws in different countries?
Mr Haley: We would not prosecute in a non-EU country, but we do have a power to prosecute within the European Union. It would make it difficult if they were breaching UK law but targeting elsewhere, outside the European Union. We could not do that because there would be no consumers in Europe who had been affected.

Q425 ***Lord Patel:*** But you just said that with spammers in the UK who had not spammed UK citizens but had sent spam to the United States we would not be able to prosecute?
Mr Haley: That is right, yes.

Q426 ***Lord Patel:*** Does that not mean the law is inadequate?
Mr Haley: If that is what the Government wanted us to do, yes, it is inadequate.

Q427 ***Earl of Erroll:*** How can you prove they did not send spam to UK citizens? A lot of citizens have "hotmail.com" as opposed to ".co.uk" accounts, which will therefore be the United States, and in fact one of my email addresses I know is hosted in Seattle. Therefore, I could well have received some of this spam.
Mr Haley: We tried very hard in that case to find consumers who had complained about this particular practice. We had to look at our own complaint database and had no complaints. We then also had the problem that we could not go into the premises of the spammers to seize any of the computers and hard drives to check who they had been spamming because our investigative powers will not stretch to that.
Earl of Erroll: In other words, I should forward all my spam on to you in future?

Q428 ***Lord Harris of Haringey:*** And your personal email address!
Mr Haley: We do have a spam OFT website where you can forward any deceptive, misleading or fraudulent spam.

Q429 ***Earl of Erroll:*** Is the problem really now that in the past, before the globalisation enabled by the Internet, a criminal had to travel to a country really to perpetrate a fraud or something of this nature, whereas now you can do it remotely across borders without ever having to leave your home ground and therefore the old principle that it has to do harm in the UK, or in the country where the person is resident, really needs to be looked at internationally and the international law? What we need is to get international co-operation on changing that principle universally?
Mr Haley: Yes, I would agree, and I also believe that our powers are still based on the off-line world of knowing where a trader is, being able to go and speak to him, have premises inspected and then take action appropriately. If we know a spamming campaign is coming over the weekend and we cannot take any administrative steps, we have to go and apply for a court order and the spam would have been sent out to millions of people before we had even had a chance to move. So I think there is a need to look at not just the international infrastructure but also for adequate powers and sanctions to apply in a fast-moving environment where I think we have lagged behind. I think Phil would agree with me about the sanctions not being really appropriate to be a deterrent for a spammer.

Q430 ***Chairman:*** There is a point which Lord Erroll made which I find very important and that is that you do seem to be comforting yourself with the fact that you do not receive as many complaints as, for example, you do for phone calls and for faxes. I think that is mainly because people do not think there is anywhere to complain to. If they knew where to complain, I think you would be drowned!
Mr Haley: I hope I did not give the impression of being comforted. I agree totally that there is a lack of a single place to complain and there are enough other direct marketing scams to keep my team busy. For us to then request information about email scams—I am sure we would be deluged if there was a simple way of electronically forwarding your complaints about email scam.

Q431 ***Chairman:*** Or even forwarding the scams?
Mr Haley: Yes, forwarding the scams. I would say also that our data on complaints does show a low incidence of people who have been victims of sending money to a spammer or giving information to a phishing site. However, we need to balance that with the fact that the economics of spamming operations mean that they only need a very small number of people to respond to make sizeable amounts of money and we should not solely base our enforcement strategies and policies based on the number of people coming forward and saying, "I've lost money." The fact that there is a spamming campaign for any product or deception means that they will be making money out of it, otherwise they would not do it. So it is a challenge to change our mindsets, if you like, in terms of whereas before we had a pile of complaints, and I have got a smaller pile here, that is an obvious case to investigate. If it is in the real world, say a direct mailing scam, we know where to go and how to do it. The other factor I would put in is that we do have a lack of skilled and competent investigators in this area to make a real dent in email and Internet scams.

Q432 ***Baroness Sharp of Guildford:*** Are there any other areas of international co-operation which we need to develop? We have more or less covered it, but you may like to add something to what you have already said.
Mr Haley: Yes. I think there are two elements to whether there should be any more international arrangements. I would put forward one as best practice. On 1 January this year the European Union brought in a new regulation on consumer protection co-operation. We have set up a network of public consumer protection agencies throughout Europe with common powers, including on-site inspections, which we lacked before, which enables information to be shared on breaches of 11 different consumer protection regulations, which include distance selling and the eCommerce regulations. It also means that we can refer cases to other European enforcement agencies to take effective action. I do not see why we could not have that also for spam-related enforcement, rather than having to look at whether it has breached those specific 11 regulations on consumer protection. On the broad issue of do we need any more kind of London Action Plans, I have a view that there are plenty of international organisations. We have the Message Anti-abuse Working Group (MAAWG), the anti-phishing working group, there is the Melbourne-Seoul memorandum of understanding, there is probably a whole list of different agencies who have an interest, different organisations and networks, and it might be time to actually look at the commonalities and having fewer of those networks. Recently in Greece six of the anti-spam agencies came together, the anti-spam networks, to have a common portal website and to try to work closer together. So I think we need a more formal network for the exchange of intelligence and effective enforcement and probably less of the informal networks set up for different cyber security threats, perhaps one covering the whole range of cyber security threats.
Chairman: Lady Hilton, did you have a question?

Q433 ***Baroness Hilton of Eggardon:*** I had a question about your 9/11 example, which seemed to me a straightforward case of fraud and I do not understand why the Americans did not apply for extradition and why it was treated as spam. It seems to me mis-labelling.
Mr Haley: It was a quite complex investigation because there was something that they were selling. They were misleading the recipients of the spam by saying, "You could be dot USA." You could be dot USA, within, I suppose the best way of putting it is on a kind of intranet. So they set up your own system, which would be like a computer's own intranet, but you could not reach your address via the World Wide Web. So it is a misleading communication in terms of the content of the spam rather than selling a dot USA web address which did not exist at all. I think this is one of the issues which in the UK would probably be dealt with by the new Fraud Act in that it is a misleading representation. Before those misleading representations would be civil matters and would rarely be investigated as fraud.

Q434 ***Earl of Erroll:*** What is the OFT's opinion of the data breach notification laws, which are common in many US states now?
Mr Haley: We do not have any particular view on those laws or in fact any breach of privacy regulations because we do not enforce the Data Protection Act or privacy regulations. We would always look to the ICO and government for a view on those types of matters.

Q435 ***Baroness Hilton of Eggardon:*** Do you see it as your responsibility to educate the public about email scams? You said there was not a single telephone point which people could communicate with. Should that not be an obvious first step, perhaps?
Mr Haley: I do believe that we have a duty to inform consumers about safe Internet shopping and how to avoid scams and spam, and in fact we have good information on our own website and on the consumer direct website, which is a service run by the Office of Fair Trading now. I think there is a whole range of organisations, local trading standards services, the Information Commissioner's Office, Internet Service Providers who have a duty to inform. I think the more information which is delivered the better, but I

think there is some work to be done about agreeing common messages so that they are reinforced and that they are simple messages which people can understand. I would encourage people to go to the OFT's website and look under consumer information and then under spam where we have got a couple of interactive games, one on phishing and one on scams and spam. I think it needs to be lively and entertaining, particularly in the on-line world, because you have to try and speak in the language of people who are on the Internet. On your very good point of whether we should have a single point of contact, I believe that people who have problems with the Internet and email expect there to be a simple electronic means of making a complaint. We do not have one at the moment. We have considered signing up to something called the 'Spot Spam' project, which is run by some European countries and is partly EU-funded, but we have not yet reached a decision on that. I think we also have to look at whether we would be overwhelmed and how we would use that information. I think there is a real opportunity for some public/private partnerships in dealing with that information because, as I said before, we are not always the most competent in terms of understanding the Internet, how it works, and tracking down the email addresses, whereas we are competent in using our investigative skills and prosecuting skills.

Mr Jones: I would just endorse Mike's comments. I think there is a multitude of people who have the responsibility for seeking to warn individuals about the risks and the things they can do to mitigate those risks if they are going to deal over the Internet. It is people who are promoting e-Government, e-business, all sorts of things. It is certainly a responsibility which we take seriously, and if I may shamelessly plug the fact that European Data Protection Day is 29 January and we will be having a re-launch of some general guidance aimed at individuals about how they can be careful about their information in relation to identity fraud but also doing business on the Internet.

Q436 ***Baroness Sharp of Guildford:*** You say you are going to be launching on that day, putting out information, and so forth. Where are you going to do this? Are you going to take newspaper advertisements, or what?

Mr Jones: We have done newspaper advertisements in the past and they are very, very expensive and we did not find them as successful as we hoped they would be. What we do have is a number of filler ads which will go on television in those spare spaces. We are hoping to drum up quite a lot of media interest and therefore hopefully get some free publicity, to be absolutely brutal, but certainly some of it will be through promoting things through media channels and certainly we will be using our website, which has fairly recently been redesigned.

Q437 ***Earl of Erroll:*** You could, of course, email all the corporate addresses!

Mr Jones: We could, of course.

Q438 ***Earl of Erroll:*** Could I just ask you very quickly about this one single point, because the police have got an under-funded fraud alert website which is run by one person who is snowed under and he is trying to do his best. Are you co-operating with them, or trying to work out which of you should be doing it, or is this an example of duplication?

Mr Haley: We work quite closely with Operation Sterling, which is the Met Police preventative strand on a number of issues, and also now with the Serious Organised Crime Agency on preventative measures. That has been a way of making interventions such as with money transfer agents like Western Union to ensure that once someone has been scammed there can be ways of preventing the money reaching the scammers. On that particular issue we have not yet talked about sharing or pooling our resources because we have not gone down the road of having a single –

Q439 ***Earl of Erroll:*** So the answer is no, because there is a chap there who is replying to 400 to 600 emails a day on frauds and it seems that there is duplication of effort there, so maybe it would be worth talking to them?

Mr Haley: We do talk to them, but I think it is the difference of what our powers would be to deal with some of the fraud. We are not fraud investigators, we only look at misleading and deceptive conduct. I know that "deception" sounds like it is fraud, but it is deception in the terms defined by the control of misleading advertising regulations. It would not be a criminal offence. I think you are right that there is more than can be done in terms of co-operation between the agencies and I will take your advice to speak with them.

Earl of Erroll: Because I do not think the consumer would know the distinction and which they should be reporting to. Until you pointed it out, I certainly did not.

Chairman: Mr Haley and Mr Jones, thank you very much indeed. It has been a valuable session for us. As I said before, if there is anything which occurs to you which you think would be of use to us, please write to us. Thank you very much.

WEDNESDAY 31 JANUARY 2007

Present	Broers, L (Chairman)	Patel, L
	Erroll, Earl of	Sutherland of Houndwood, L
	Hilton of Eggardon, B	Young of Graffham, L
	Mitchell, L	

Memorandum by Symantec

Symantec welcomes the opportunity offered by the Science and Technology Committee to submit evidence on security issues affecting private individuals when using communicating computer-based devices, either connecting directly to the Internet, or employing other forms of inter-connectivity.

I. Defining the Problem

What is the nature of the security threat to private individuals? What new threats and trends are emerging and how are they identified? What is the scale of the problem?

- The nature of security varies from attacks on technical vulnerabilities to social engineering techniques (virus, worms, spyware, phishing);
- The emergence of new technologies such as Instant Messaging (IM), VoIP etc., create new potential platforms for e-crime. For example, IM, one of the most successful and widely deployed applications on the Internet, has become a potent means of propagation of viruses, worms and other threats. It is also particularly well suited for social engineering tactics and in the case of young users, for grooming for paedophilia as it is a tool which tends to be inherently trusted by users. As IM moves to Voice and Video, the scope of risk of child exposure to harmful content may increase. Parental control and level of access could be included to protect children from these emerging risks;
- Shift from attacks motivated by notoriety to attacks motivated by economic gain: Private individuals are increasingly targeted by phishing scams and spyware designed to steal confidential information and pass it along to attackers;
- Fraud and theft: as rewards get more attractive, attackers will continue to improve their methods: volume and severity of attacks continues to rise from noise categories 3&4[1] attacks to quieter, stealthier category 1 &2[2] attacks;
- Increased Threats to e-Commerce: During the last semester 2005, e-Commerce was the single most targeted industry, with nearly 16 percent of attacks against it. This represents a 400 percent increase from the 4 percent reported during the previous six months;
- Attacks against web application technologies are increasingly popular: Web application technologies are appealing targets for attacks because of their widespread deployment within organisations and the relative ease with which they can be exploited. Web applications allow attackers to gain access to the target system simply by penetrating one end-user's computer, bypassing traditional perimeter security measures. Nearly 82 percent of documented Web application vulnerabilities were classified as easy to exploit, thereby representing a significant threat to an organisation's infrastructure and critical information assets;
- Time Between Vulnerability and Exploit is shortening: According to the report, the time between the announcement of a vulnerability and the release of associated exploit code was extremely short. Symantec data[3] indicates that over the past six months, the average vulnerability-to-exploit window was just 5.8 days. Once an exploit has been released, the vulnerability is often widely scanned for and

[1] Symantec uses a threat matrix to categorise the different level of threat posed by malware. The categorisation within that matrix ranging from 1 (least severe) to 4 (most severe) Is determined by a number of factors, such as the ease of infection, the speed of propagation, the damage caused etc.

[2] Idem as 1.

[3] cf Symantec Internet Security Report, Trends for July 2005 to December 2005, Vol IX, March 2006.

quickly exploited. This short window leaves organisations with less than a week to patch vulnerable systems;

— Bots and Bot Networks and customisable or "modular malicious" code are the preferred method of attack. Adding to concern about the short vulnerability-to-exploit window is the growth in bots (short for "robot"). Bots are programs that are covertly installed on a targeted system, allowing an unauthorised user to remotely control the computer for a wide variety of purposes. Attackers often co-ordinate large groups of bot-controlled systems, or bot networks, to scan for vulnerable systems and use them to increase the speed and breadth of their attacks. Over the past six months, Symantec has seen a large increase in the number of remotely controlled bots. During the first six months of 2004, the average number of monitored bots rose from under 2,000 to more than 30,000 per day—peaking at 75,000 in one day. Bot networks create unique problems for organisations because they can be remotely upgraded with new exploits very quickly, which could potentially allow attackers to outpace an organisation's security efforts to patch vulnerable systems; and

— Increase in Severe, Easy-to-Exploit Vulnerabilities: Symantec documented more than 1,237 new vulnerabilities between January 1 and June 30, 2004, an average of 48 new vulnerabilities per week. Seventy percent of these vulnerabilities were considered easy to exploit, and 96 percent were considered moderately or highly severe. Consequently, organisations must contend with an average of more than seven new vulnerabilities per day, and a significant percentage of these vulnerabilities could result in a partial or complete compromise of the targeted system.

Attack Trends:

— The Slammer worm was the most common attack for the last semester of 2005, with 15 percent of attacking IP addresses performing an attack related to it. Gaobot and its variants were the second most common attack, increasing by more than 600 percent over the past six months;

— Overall, the daily volume of attacks is decreasing due to a decline in Internet-based worm attack activity over the first six months of 2004. E-Commerce received the most targeted attacks of any industry during this period; small business received the second most; and

— The United States was the top attack source country with 37 percent, down from 58 percent in the previous six months. Other countries rose accordingly, indicating that attack activity is becoming more international. UK remains the top originating country for bot-attacks (7 percent of worldwide bot-attacks) probably due to the implementation of Broadband, which is not adequately secured;

Vulnerability Trends:

— During the first six months of 2004, the average time between the public disclosure of a vulnerability and the release of an associated exploit was 5.8 days;

— The Symantec Vulnerability Database documented 1,237 new vulnerabilities between January 1 and June 30, 2004. Ninety-six percent of documented vulnerabilities disclosed during this period were rated as moderately or highly severe; 70 percent of vulnerabilities were considered easy to exploit; 64 percent of vulnerabilities for which exploit code is available were considered high severity; and

— In the first half of 2004, 479 vulnerabilities—or 39 percent of the total volume—were associated with Web application technologies.

Malicious Code Trends:

— Over the past six months, Symantec documented more than 4,496 new Windows viruses and worms (particularly Win32), more than 4.5 times the number in the same period in 2003;

— The number of distinct variants of bots is rising dramatically, increasing by 600 percent over the past six months;

— Peer-to-peer services (P2P), Internet relay chat (IRC), and network file sharing continue to be popular propagation vectors for worms and other malicious code;

— Adware is becoming more problematic, making up six of the top 50 malicious code submissions; and

— The first malicious worm for mobile devices, Cabir, was developed.

Future and Emerging Trends:

— User-side attacks are expected to increase in the near future. Targeted attacks on firewalls, routers, and other security devices protecting users' systems are also a growing security concern;

— Symantec expects bot networks to employ increasingly sophisticated methods of control and attack synchronisation that are difficult to detect and locate. Symantec also expects to see instances of port knocking, a method attackers may use to create direct connections to potential target systems; and

— Symantec expects that recent Linux and BSD vulnerabilities that have been discovered and used in proof-of-concept exploits will be used as exploit-based worms in the near future. Symantec also expects to see more attempts to exploit mobile devices.

How are security breaches affecting the individual user detected and recorded?

There are a number of technologies available to detect and record security breaches and attacks. These are employed in different ways by different users. For example the average consumer who is using a security solution on his or her PC like the Symantec Internet Security suite will have a set of log-files generated every time there is malicious activity detected. In addition the user will be receiving pop-up messages from the Symantec security solution informing him about the attack and the measures taken to protect the system and how its status is affected. Similar log-files and messages to the user or the system administrator are generated by different Symantec security solutions installed in enterprise environments. In addition there exists specialised sensor technology employed by the Symantec early warning system (Deepsight) which is designed to record attacking activity and provide early warning information and intelligence on attacks. Another technology is employed by Symantec Managed Security Services which monitor using sensors real-time customer systems and alert the system administrator for attacks on its system or can even take precautionary measures to prevent a system compromise.

The UK government through DTI is also conducting an e-crime and breach survey which Symantec has sponsored.

Hence it is evident that there are a number of technologies suitable for different environments and different user-sophistication that afford adequate level of information and warning for attacks.

How well do users understand the nature of the threat?

There is a lack of awareness about the current level of information security threats. Users and enterprises depending upon their level of sophistication, economic capacity and their risk profile will understand or not the problem and will take or not relevant measures. The average consumer or SME are probably the ones with the least knowledge around this issue which makes them probably most vulnerable, due to a large extent to the proliferation of broadband connectivity. It is therefore welcomed that the UK Government, in conjunction with a number of private sector entities, is conducting awareness-raising activities like the Get Safe Online campaign. The European Union has also underscored the importance of awareness raising on its recent Communication[4] on information security. Awareness raising is also one of the tasks of the European Network and Information Security Agency (ENISA) that recently issued a toolkit[5] for governments on this topic.

II. Tackling the Problem

What can and should be done to provide greater computer security to private individuals? What, if any, are the potential concerns and trade-offs?

— A role for intermediaries: In order to address computer security to private individuals effectively it is necessary to address it from a global standpoint and lay out a multi-layered defence against attacks. Security remains ultimately also a user responsibility and the end-to-end nature of the Internet cannot and should not be challenged. However, as an increasingly complex and constantly evolving threat landscape unfolds, private users cannot be expected to guarantee their security online alone. Upstream defence is necessary. For instance, electronic communication service providers can play a key role in addressing information security threats as a first line of defence;

— Competition as a guarantee for security: Diversity in software platforms and applications is key to containing the spread of security threats such as malware and viruses. A monoculture in software applications would entail that a single point of failure would affect users globally. Promoting a competitive market for security software industry protects diversity and thereby enhances security;

— Early warning and intelligence collection: Layered defence entails anticipation. Tracking security events on a global basis can enable early warning of upcoming active attacks. This allows users to be alerted and prepared at best against a potential attack; and

[4] http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006—0251en01.pdf

[5] http://www.enisa.eu.int/doc/pdf/deliverables/enisa—a—users—guide—how—to—raise—IS—awareness.pdf

— Raising awareness and User Best practice (c.f annex 1): User awareness of the threat and of the means to address it is as important as computer technical protection. As networks and computers become more secure, hackers turn to the weakest link, the individual user (for example: phishing scams). Educating the user to use information communications technology responsibly is therefore as important as protecting the machine;

There is a role for business and government to play and collaborate in this respect. Public/private partnership fora can help establish and monitor best-practice standards. Awareness-raising tools include training in the workplace and via easy-to-use public access web sites where users can learn and also share experiences. The media can also be enlisted to publicise the importance of safe cyber practices. Symantec has drawn up a list for user's best practices enclosed at annex 1.

What is the level of public awareness of the threat to computer security and how effective are current initiatives in changing attitudes and raising that awareness?

It is somewhat effective provided that awareness campaigns take place and that there is a follow up to those activities. Public-private partnerships among government and industry have a key role to play in this area.

What factors may prevent private individuals from following appropriate security practices?

Lack of awareness of the potential danger is a main factor which prevents private individuals from following appropriate security practices.

What role do software and hardware design play in reducing the risk posed by security breaches? How much attention is paid to security in the design of new computer-based products?

More and more attention is paid to the security when designing new IT products, although often until the level of threat and the risk profile is well-understood, it may not always be straight forward to adequately assess the level of security required for new products. A good example of that could be VoIP technologies which have been originally designed with quality of services as a primary consideration. The more VoIP communications proliferate, the more security and confidentiality of those communications will become a key issue. At the same time, it is important for policy-makers to ensure that security should not be used as an argument for anti-competitive practices (such as intentional refusal to disclose information related to interoperability) when putting into market a new product. Diversity, innovation and competition are key drivers for security which would be hampered if there cannot be competing security solutions on the different technology platforms.

Who should be responsible for ensuring effective protection from current and emerging threats?

There cannot be a single entity held accountable. The nature of the internet and IT technology is such that no single person can be held accountable.

III. Governance and Regulation

How effective are initiatives on IT governance in reducing security threats?

Often security is seen more as a cost and less as a business enabler. Regulatory compliance therefore is often seen as a key driver for information security being placed high in the agenda of IT governance. Examples include regulations on data protection, SOX, data retention and Basel II.

How far do improvements in governance and regulation depend on international co-operation?

Considerably. EU-US co-operation is critical in this area. Frequently regulations issued by either side will cascade to the business environment of the other, having extra-territorial effects. Examples in this area include data protection for Europe and SOX for the US. These create major compliance challenges and a patchwork of regulations that increase costs and inefficiency.

Is the regulatory framework for Internet services adequate?

The regulatory framework for Internet services within the meaning of Electronic Communications, Information Society services and E-Commerce, is probably adequate. However when it comes to information security, with the exception of some criminal law provisions and data protection, there is no specific information security regulatory framework.

What, if any, are the barriers to developing information security systems and standards and how can they be overcome?

It is important to ensure strong intellectual property protection to the developers of information security technology so as to create research and investment incentives in this fast growing and changing arena.

It is important to ensure software quality by improving the current Common Criteria certification process in terms of technological quality as well as in terms of cost reduction. The cost element is particularly important in allowing new entrants in the market. It is important to ensure that there are no competing certification or standardisation schemes to Common Criteria because this will increase the costs of creating secure technologies that are commonly accepted across a number of jurisdictions.

It is also important that there are no technology mandates introduced for security because that could stifle innovation and ultimately achieve opposite than the desired results in terms of protection.

Finally it is of paramount importance for reasons previously explained to ensure a functional and competitive marketplace whereby users and consumers will have choice about the technologies they wish to use and providers have access to the necessary information to compete in developing high-quality and innovative security products.

IV. Crime Prevention

How effective is Government crime prevention policy in this area? Are enforcement agencies adequately equipped to tackle these threats?

The UK is probably among the best placed countries in comparison to several other EU Member States in countering cybercrime. However, there is certainly room for improvement by providing more training and more resources to the UK police. Strong collaboration with the private sector in this area is a key success factor as it is the private sector that controls the infrastructure and has most knowledge about the threats. Recently the NHTCU was incorporated into SOCA. It remains to be seen how this will affect the enforcement activities.

Is the legislative framework in UK criminal law adequate to meet the challenge of cyber-crime?

The CMA is currently before the House of Lords for updating. There is probably consensus about the need to update the CMA and, in general, it is fair to say that the business community probably shares the objectives that the amendments proposed by the government aim to achieve. However, some questions have been raised by industry regarding the wording proposed for some of the CMA amendments. It is felt that the language proposed could be improved so as to ensure a higher level of legal certainty.

How effectively does the UK participate in international actions on cyber-crime?

UK is active in international forums and is known to be an effective counterpart. The UK is active in the G8 and in the EU. However, unlike the US which recently ratified the Council of Europe Convention on cybercrime, the UK has still to do so despite having signed it. There is strong business support for the ratification of the Convention as it is by far the most comprehensive legal instrument in the fight against cybercrime.

Annex 1

USER'S BEST PRACTICES

1. Use an Internet security solution that combines antivirus, firewall, intrusion detection, and vulnerability management for maximum protection against malicious code and other threats.

2. Ensure that security patches are up-to-date and that they are applied to all vulnerable applications in a timely manner.

3. Ensure that passwords are a mix of letters and numbers. Do not use dictionary words. Change passwords often.

4. Never view, open or execute any email attachment unless the attachment is expected and the purpose of the attachment is known.

5. Keep virus definitions updated regularly. By deploying the latest virus definitions, private users can protect their computers against the latest viruses known to be spreading "in the wild".

6. Private users should routinely check to see if their PC or Macintosh system is vulnerable to threats.

7. All computer users need to know how to recognise computer hoaxes and phishing scams. Hoaxes typically include a bogus email warning to "send this to everyone you know" and/or improper technical jargon that is intended to frighten or mislead users. Phishing scams are much more sophisticated. Often arriving in email, phishing scams appear to come from a legitimate organisation and entice users to enter credit card or other confidential information into forms on a Web site designed to look like that of the legitimate organisation. Computer users also need to consider who is sending the information and determine if the sender is a trustworthy, reliable source. The best course of action is to simply delete these types of emails.

8. Private users can get involved in fighting cybercrime by tracking and reporting intruders. With Symantec Security Check's tracing service, users can quickly identify the location of potential hackers and forward the information to the attacker's Internet service provider or local police.

9. Be aware of the differences between adware and spyware. Adware is often used to gather data for marketing purposes and generally has a valid, benign purpose. Spyware, on the other hand, may be used for malicious purposes, such as identity theft.

10. Both spyware and adware can be automatically installed on a computer along with file-sharing programs, free downloads, and freeware and shareware versions of software, or by clicking on links and/or attachments in e-mail messages, or via instant messaging clients. Therefore, users should be informed and selective about what they install on their computer.

11. Don't just click those "Yes, I accept" buttons on end-user licensing agreements (EULAs). Some spyware and adware applications can be installed after an end user has accept the EULA, or as a consequence of that acceptance. Read EULAs carefully to examine what they mean in terms of privacy. The agreement should clearly explain what the product is doing and provide an uninstaller.

12. Beware of programs that flash ads in the user interface. Many spyware programs track how users respond to these ads, and their presence is a red flag. When users see ads in a program's user interface, they may be looking at a piece of spyware.

Memorandum by MessageLabs

Addressing the security issues affecting private individuals when using the Internet is crucial to building and maintaining a stable and successful online economy in the UK. The current rapid growth and convergence of spam, viruses and spyware threats has shown the priority given by the Select Committee to these issues to have been particularly timely and prescient.

Only through efficient and proportionate responses to the threats presented by spam and viruses, will citizens overcome their online security fears and grasp the opportunities offered by the Internet. It is therefore important to understand the nature of the very latest online threats, and that any possible doubts regarding privacy aspects of filtering technology be addressed in as comprehensive a way as possible.

As the world's leading provider of third party filtering for spam and viruses, MessageLabs has been privileged to be involved in numerous consultations on this and related network security issues, both in the EU and US and also through the OECD.

Defining the Problem

The very latest security threat that MessageLabs has been tracking is also perhaps one of the most significant threats in recent years; namely, that of the "targeted trojan". Each targeted trojan is a "one off", a unique piece of malware created with the express intention of breaching a single organisation or even an individual, for stealing personal data, intellectual property or other sensitive information. Since such trojans are "one offs" the probability of them ever making it onto the radar of the broader security community are practically zero. Each targeted trojan is deployed to a limited number of carefully selected targets, typically one attack, comprising of around 7 emails per day are intercepted by MessageLabs, an increase from one attack every two

to three days. However, traditional anti-virus security companies can only safeguard against the threats that they know, and have little chance of protecting against a genuinely new virus or trojan.

Over the past three years, almost all viruses and spyware have been created for commercial and criminal gain. These viruses are continually being used to create robot-networks ("botnets") of compromised PCs around the world, and these are in turn harnessed by the online criminals for hire by spammers and other unscrupulous networks. Botnets may be used to attack online businesses using a co-ordinated "distributed denial of service" attack, or may equally be used to send millions of spam emails per hour, from each individual PC, using what is known as a "spam cannon" or essentially the spammer's equivalent of a distributed mail-merge, on a grand scale.

Spam

In September 2006, the global ratio of spam in email traffic from new and unknown bad sources, for which the recipient addresses were deemed valid, was 64.4 percent (1 in 1.55 emails), a decrease of 0.1 percent on the previous month. This figure of 64.4 percent is actually a lower than the "true" spam figure. In early 2005, MessageLabs deployed an additional layer of defence at its network perimeter, known as Traffic Management. This enables us to control the amount of bandwidth that we give to absolutely known bad-sources of spam, and then to throttle those connections, slowing them down to a crawl so that to the spammer, they appear to be talking to a very slow modem. Consequently, many such connections eventually "time-out" or move on to softer targets. If we look at the amount of spam hitting our honey-pots, which are unprotected by comparison, this figure would be much closer to 82.1 percent.

In recent weeks, MessageLabs has noticed an increase in the number of spam emails that use "techno-babble" usually only associated with particular technology strands as a means of social engineering. Not only do messages with enticing subject lines, such as "Bug £33006: Your review is necessary," find their way into programmers' inboxes, but there is also a suggestion that these emails may be deliberately targeted so as to be appealing to these particular groups. In another twist, the "geek" demographic seems to be particularly susceptible to this type of spam, in that the Bayesian filters so often employed by such techies can be easily polluted with technology buzzwords secreted into the body of the spam, such as ".NET" "CPAN" "XSS" "Java" etc.

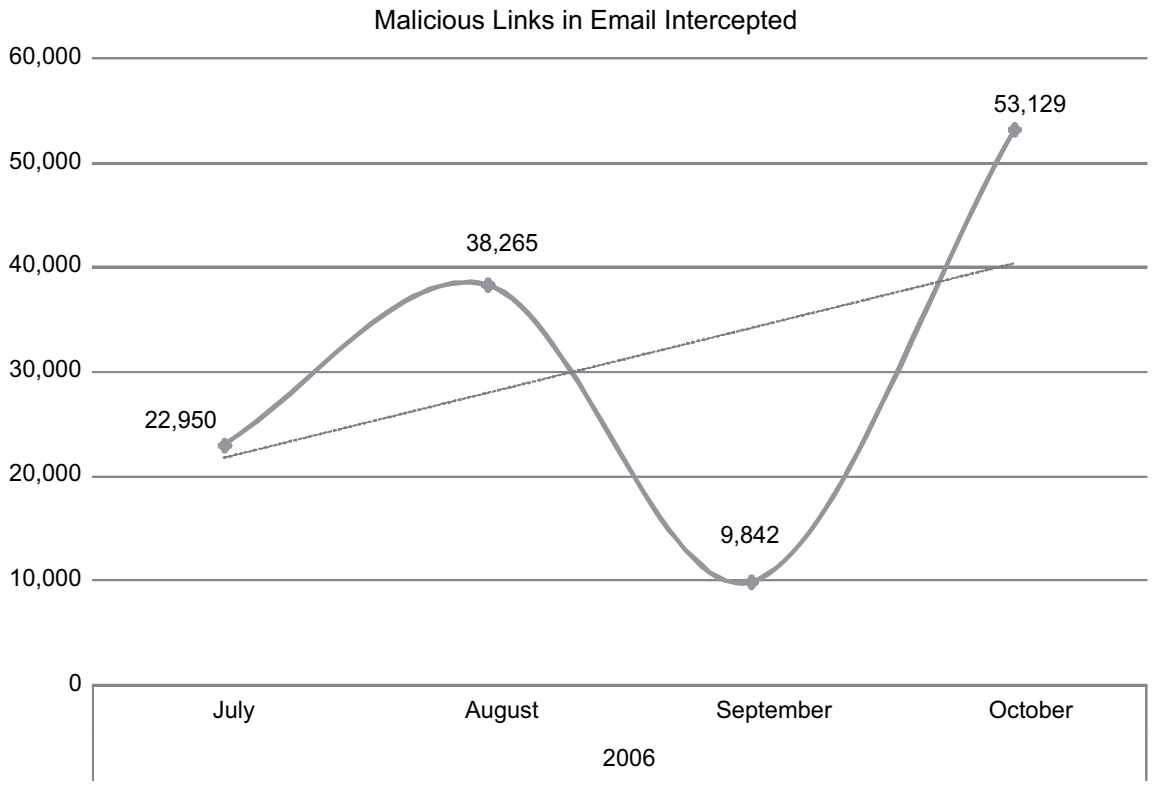
Viruses, Trojans and Other Malware

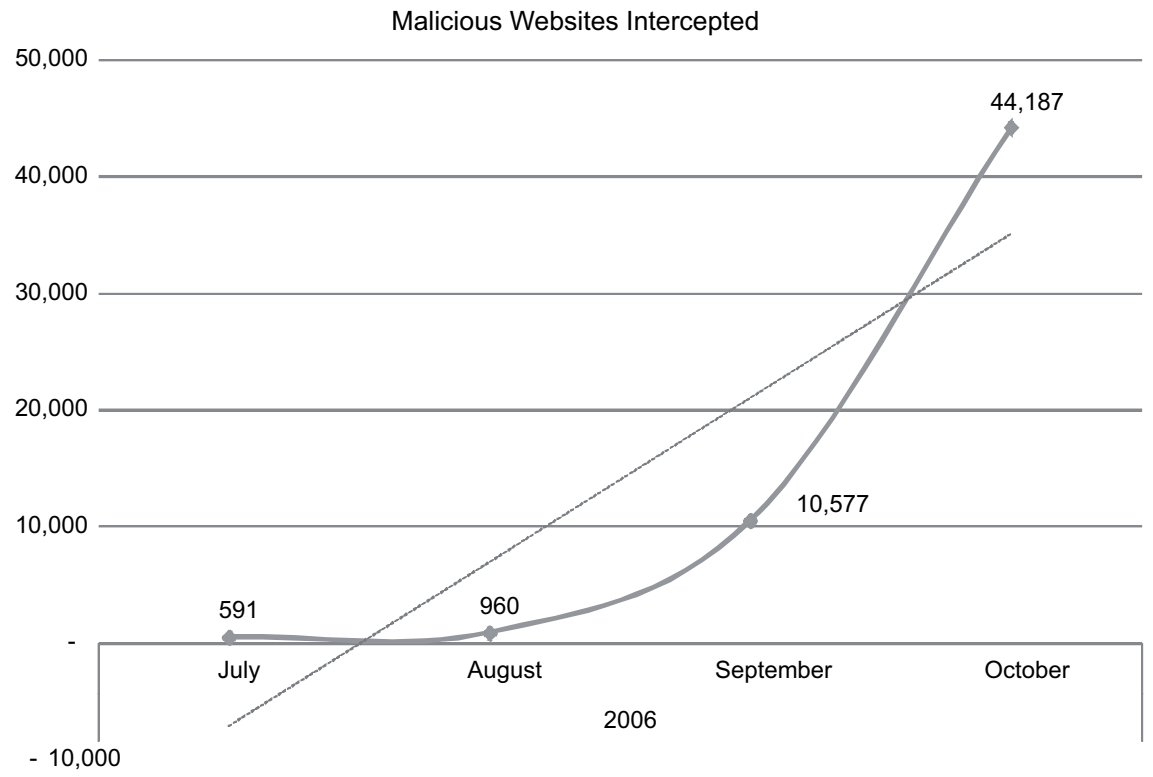
The global ratio of email-borne viruses in email traffic from new and previously unknown bad sources destined for valid recipients, was 1 in 89.6 emails (1.12 percent) in September, an increase of 0.1 percent since last month.

In 2006, MessageLabs has also seen a marked shift in the way online criminals are distributing their malware, in that the proportion of executable-type attachments has declined. This has given way to more social engineering attacks, like phishing.

The convergence of emails threats and the web as a medium have led to an increase in the number of emails containing links to websites hosting malicious software. The malicious website then becomes the vehicle by which the malware is installed onto victims' computers.

This is highlighted in the charts below:





Botnets

A "Botnet" is a collection of compromised computers around the world, infected with trojan horses, or backdoor software, and united by a common command and control infrastructure. A botnet's controller ("bot herder") can control the group remotely, en masse. It can be seen from the following table that bots are increasing in number and distribution:

Botnets by geography

		Q2 2006	Q3 2006
Top10	United States	10.1%	11.3%
	China	9.5%	7.4%
	Uruguay	3.5%	6.8%
	India	8.4%	6.2%
	United Kingdom	5.2%	4.8%
	France	4.8%	4.8%
	Germany	4.5%	4.6%
	Brazil	2.8%	4.4%
	Poland	2.9%	3.8%
	Taiwan	3.1%	3.4%
Total botsglobally			2.8 million

This shows that over the last two quarters in 2006, the UK has remained fifth in the top-ten list of botnet-infected regions. However, it is encouraging to note that the percentage of botnet-infected computers in the UK has dropped by 0.4 percent.

This percentage representing the proportion of "bots" worldwide, ie 134,400 estimated computers in the UK are currently participating in a botnet of some kind. Botnet computers are typically high-bandwidth (DSL connected) home computers, with little or no protection in place.

Phishing

September 2006 showed a large increase of 0.27 percent in the proportion of phishing attacks compared with the previous month. One in 170 (0.59 percent) emails was some form of phishing attack. When judged as a proportion of all email-borne threats such as viruses and trojans, the number of phishing emails has risen by 21.7 percent. Phishing attacks accounted for more than half (52.4 percent) of all malicious emails intercepted by MessageLabs in September.

Phishing attacks continue to become more targeted as more criminal groups shift their attention from creating malware to conducting phishing attacks. The nature of these attacks has also changed in recent months, as the main organisations now being targeted have become those banks that have not currently deployed any two-factor authentication security measures. The approach undertaken by some banking organisations has indirectly resulted in a huge increase in the phishing attacks directed against those banks that may be delaying implementation or still investigating such technology. Those banks that have deployed this technology are still being subjected to attacks, but on a much lesser scale.

These increased attacks were also a prelude to the release of Microsoft Internet Explorer 7.0, which was launched in October. IE7 includes additional anti-phishing countermeasures. Already, MessageLabs has seen examples of specially crafted bank trojans that are being sold on the Internet, which can be customised for as little as US $800 to target any online banking website. The trojan approach works by monitoring browser addresses and when the victim visits a target site, the trojan will wait for the user to complete the authentication process before hijacking the session and handing control to the criminals.

Web

In the table below it can be seen that the most common trigger for policy-based filtering, applied by MessageLabs for its business clients, is Advertisements & Popups (90.1 percent).

WebSecurity Services (Version 2.0) Activity:

Policy-BasedFiltering		Web Viruses and Trojans		Potentially Unwanted Programs	
Advertisements & Popups	90.1%	Trojan-Clicker.HTML.Agent.a	35.4%	Adware-180SA	409%
Streaming Media	3.3%	Generic Downloader.o	13.5%	Adware-ISTBar	34.8%
Downloads	1.2%	JS/Wonka	10.2%	Adware-Lop	6.1%
Unclassified	1.2%	Trojan-Downloader.HTML.Agent.aq	5.6%	Adware-GAIN	6.1%
Adult/Sexually Explicit	0.8%	W32/VBS_Malware	5.2%	Adware-Look2Me	3.0%
Web-based E-mail	0.5%	Suspicious IFrame-c	1.6%	Adware-abetterintrntdldr	3.0%
Chat	0.5%	Trojan-Downloader.Win32.Agent.alr	1.5%	Adware-UCMore	1.5%
Shopping	0.4%	Trojan-Downloader.JS.Agent.ac	1.5%	Adware-PurityScan	1.5%
Blogs & Forums	0.4%	Trojan-Downloader.Win32.Small.cpg	1.3%	Adware-abetterintrnt.gen.a	1.5%
Personals & Dating	0.3%	Trojan-Downloader.JS.Agent.ap	1.2%	Adware-ISTbar.b	1.5%
Other	1.4%	Other	23.0%		

The "Unclassified" category identifies new and previously uncategorised sites that may potentially need to be prohibited. The "Unclassified" category affords more confidence when defining new rules, which means that newly detected malicious sites may be handled more appropriately until categorised, thereby safeguarding against sites which appear and disappear within a 24 to 48 hour timeframe; such sites may be used for disreputable purposes, such as hosting phishing and spam sites, information stealing trojans and other fraudulent activities.

Analysis of web security activity also shows that 99.7 percent of interceptions occur as the result of a rule triggered by a policy, which has been implemented by a system administrator. However, 0.3 percent of interceptions are also the result of malware or potentially unwanted programs, including adware and spyware that was detected heuristically by MessageLabs.

Summary

In the short-term, a high-degree of vigilance can prevail against some of the more contemporary attacks, but only for so long. As cyber criminals become more organised and highly developed, attacks are becoming more targeted, using social engineering to bypass technological barriers. Even the most cautious amongst us may fall prey to such an attack; curiosity in humans, as in cats, can have a very powerful and dangerous influence—sometimes overtaking any consideration for safe computing practices. Accordingly, businesses and individuals alike must consider the primary conduit through which these threats flow in order to mitigate them effectively.

To do this securely, the principal security defences should be concentrated on these ingress points rather than at the desktop—where often it can already be too late when a breach occurs. Taking this to another level, protocol independent defensive countermeasures woven into the fabric of the internet itself will become the key component of any services-orientated solution. In the same way, domestic broadband connections are the most heavily abused in terms of botnet dispersion, and in turn home users will be looking to their ISP to provide solutions at the Internet level itself.

Over time, legislation and enforcement in this area will improve and through greater international co-operation and co-ordination it will become much more difficult for the cyber criminals to exploit the differences in cross-border jurisdiction. However, this is fundamentally a technical problem and as such will always require a technical solution, first and foremost, and by addressing the problem "in the cloud" at the Internet level, it is taking the fight one step closer to the criminals.

23rd October 2006

Examination of Witnesses

Witnesses: MR ROY ISBELL, Vice-President, Symantec Global Government Services, MR ILIAS CHANTZOS, Head of Government Relations for EMEA, Symantec, MR MARK SUNNER, Chief Security Analyst, and MR PAUL WOOD, Senior Analyst, MessageLabs, examined.

Q440 ***Chairman:*** Welcome everybody to this session of the Science and Technology Select Committee. I would like to particularly welcome our witnesses. Thank you for your time and for what you have submitted to us already. Members of the public who are here, you will be aware that there is a notice which you can pick up about this meeting and the mission we have on the Select Committee in this inquiry. Perhaps I could ask the witnesses first to introduce yourselves and then, if you wish, make an opening statement. Perhaps, Mr Isbell, we could start with you?
Mr Isbell: Certainly. I am Roy Isbell. I am the Vice-President of Global Government Services for Symantec.
Mr Chantzos: My name is Ilias Chantzos. I am the Head of Government Relations for Europe, the Middle East and Africa of Symantec Corporation.
Mr Wood: My name is Paul Wood. I am the Senior Analyst at MessageLabs.
Mr Sunner: My name is Mark Sunner. I am the Chief Security Analyst, MessageLabs.

Q441 ***Chairman:*** Thank you very much. Do any of you wish to make an opening statement?
Mr Isbell: My Lord Chairman, I would like to make a statement from Symantec, if I may. Symantec extends its thanks to the Committee for the opportunity to provide oral evidence in this inquiry. We welcome the opportunity to answer your questions and further the position outlined in our written submission to the Committee. In September Symantec published its latest Symantec Internet Security Threat Report from data collected on security attacks between January and June 2006. Our findings showed the UK with the third highest number of bot infected computers worldwide and the third most targeted country for denial of service attacks. The UK is also fourth in the world for spam creation with 4 per cent of the world's spam originating in the UK. The report also confirms that home users are the most targeted online with 86 per cent of attacks aimed at the individual home users. Symantec believes all stakeholders should strive to improve security at all levels given the ever-evolving online threat environment. An effective information security policy relies on a multi-layered defence against attacks. Whilst security remains ultimately users' responsibility, as an increasingly complex of threats emerge Symantec understands users cannot be expected to ensure an adequate level of security on their own. Symantec is committed to developing solutions which help individuals ensure the security, availability and integrity of their information.

Q442 ***Chairman:*** Thank you very much. Would anybody else wish to make a statement?
Mr Sunner: I would just like to also reiterate and extend our thanks for the opportunity to give evidence here. We ourselves at MessageLabs are an Internet-based security company. The premise is to filter traffic en route to our customers at the Internet level rather than at premises, and for that we filter email, web traffic and instant messaging. During the latter half of 2006 we have observed some interesting trends in trojan and spam-related activity which are unprecedented from a technical perspective and we would like to share some of the trend information which we have with you today.

Q443 ***Chairman:*** Thank you very much. We have quite a long list of questions. I would ask you, if possible, to be succinct in your answers and to speak up because the acoustics in this room are not good. Let me ask the first question, which is a very general question. How much email spam is being sent?
Mr Sunner: Currently, heading towards the corporate world, 75 per cent of all email now heading towards companies is spam. For the domestic populace that is closer to, conservatively, about 85 per cent.

Q444 ***Chairman:*** 85 per cent of the total is spam?
Mr Isbell: That is slightly different from the measurements which we made. In our measurements, according to the period in question, spam made up 54 per cent of all monitored email traffic which we were able to monitor, and that was up from 50 per cent in the previous period.

Q445 ***Chairman:*** That leads me to my supplementary question: how accurate do you think these numbers are? We have already had an interesting spread.
Mr Isbell: I think it depends on the reach of the intelligence network the organisation has which is actually measuring it. Currently we monitor 30 per cent of the global email traffic which goes through the Internet.

Q446 ***Chairman:*** 30 per cent?
Mr Isbell: 30 per cent of all email traffic goes through our botmail facility.

Q447 ***Chairman:*** Spammers send different amounts of spam to different people and presumably can tell who is being protected by filtering systems and send more or less spam accordingly. Is this so, and if so how does it affect the accuracy of these overall figures?

Mr Isbell: We are seeing increased targeted attacks of spam, that is definite, if I could answer the question in that way. The effectiveness of their monitoring is unknown to us at this moment in time. The spam we are actually witnessing is; products 26 per cent, adult spam 22 per cent, and commercial products 19 per cent of the total spam make-up. So to directly answer your question, we are seeing a degree now of targeted spam through social engineering, depending on particular events which might be happening. A particular case in point which comes to mind is St Valentine's Day which is now coming up, so we are seeing targeted events around St Valentine's Day to get people to open up that spam.

Mr Sunner: Just to go back to the numbers, we have seen the profile of spam actually change quite significantly in the last three years. Three years ago we were seeing the volumes of spam back then were about 50 per cent. Now we see it at 75 per cent and that is based on us clearing nearly 2 billion emails per week. Within the profile of that spam, again to come back to the targeted nature, what we have seen is that whereas the biggest arsenal of the spammer used to be to just send more of it, now they are attempting to profile who it is heading towards. So we see spam targeting particular demographs or people who use certain banks in terms of phishing, and one of the alarming aspects of this is how they are able to do this. 2006 saw a huge rise in the use of social networking sites. These are websites such as My Space where people willingly key in a lot of information about themselves which the spammers, and more importantly phishers, are then able to plunder this information and make their attacks more focused, which means they are more socially engineered, which means people are more likely to click on these things. That is probably the biggest profile, not just within the growth of the volume we are seeing but the change of behaviour within the messages which are coming out.

Q448 ***Chairman:*** Do you think we are going to win this battle of being able to filter spam, or do you think spammers will just be able to make it invisible?

Mr Sunner: Clearly this is an arms race, so it will consistently be a moving target, but I think the more we can interweave the detection and the filtering of this content into the fabric of the Internet—and that is not just for email, that goes for web traffic and instant messaging as well—dealing with it "in the cloud" as opposed to at the end point, the same as a utility model—in the same way as you would not expect to have to boil your own water at home before you could use it, clearly that would be mad, but in IT that is what everyone is doing with their email. So if you can get the detection into "the cloud" you can be much more aggressive about how you can filter this stuff out and you are also a stage closer to the source of the problem, which also helps in potentially tracking this down and eliminating the botnets.

Mr Isbell: I would also agree that a multi-layered defence approach is required. I fully agree with my colleague about getting it into "the cloud", but effective end point security to filter at the end point is also a requirement.

Q449 ***Baroness Hilton of Eggardon:*** How much of all this spam is actually carrying viruses? Have you any idea of the proportion?

Mr Sunner: I can tell you that currently for January one in every 119 messages on average that we are processing contains a virus that is a trojan of some description. The vast majority, over 90 per cent, are botnet related. So the vast majority of viruses are actually to do with spam. They are essentially the air supply for spammers, where the target is home users rather than business. That number is actually down from January 2006, where the number would have been closer to approximately one in 250 –

Mr Wood: It would certainly have been a lot lower, I think.

Mr Sunner: What used to happen was that the volume of viruses was directly linked to the volume of spam, so if we saw more viruses we knew more spam would follow it, and that de-coupled about July 2006. What this means is the bots which are going out there are now much more efficient at sending spam. So the bad guy community, for want of a better word, is interested in sending more discrete viruses which stay under the radar for longer, which go undetected for longer by companies like ourselves, so that they can basically have a longer existence. We believe this trend will continue, that the virus count will actually continue to come down in email but go up inside web traffic, but spam volumes will continue to go up the whole time. That is exactly the trend we are seeing at the moment.

Mr Isbell: That concurs with our findings, that one of every 122 spam messages is blocked by our botmail system containing malicious code. Our probe network also detected 157,477 unique phishing messages during that period.

Q450 ***Lord Sutherland of Houndwood:*** Can I ask what you mean by "unique"?

Mr Isbell: These are distinct in their own right. They are all separate and distinct in what they are trying to do.

Q451 ***Lord Sutherland of Houndwood:*** To follow through, you obviously have a huge experience of what the bad guys are doing. You also want to look on the other side at which the consumers, those who have systems, need. Do you think they are getting enough education about the dangers out there on the net? If so, fine—I suspect not—but if not, what would you suggest?

Mr Isbell: We did think about this and we have had some internal discussion going on about this. Education and awareness is a multi-faceted and multi-targeted environment. I do think there is the opportunity to give more education for our children under the ICT programme for schools. We all know that these are the surfers of the future and we also know that children in our environment teach mum and dad how to use the video recorder remote, so I think that raising the level of education regime and the level of awareness in our children is one way forward to improve overall. Secondly, I think we also need to be aware that we are getting an increased number of what are known as "silver surfers", an ageing population.

Q452 ***Lord Sutherland of Houndwood:*** I think you have some around the table in front of you!
Mr Isbell: I do not think we are actually doing enough to target that demographic because they need more help, I believe, than somebody in their mid-term.

Q453 ***Lord Sutherland of Houndwood:*** I can follow that. There is a bit of tension here because clearly one of the things one wants to do is encourage more people, not least the potential silver-surfers, to use this capacity to enlarge their lives, but if at the same time you frighten the wits out of them—is there a tension there which you are noticing or experiencing?
Mr Isbell: I think there is a danger that we could go too far down the fear, uncertainty and doubt route (the FUD factor, as it is called), but I think if the awareness and training is done in a sensitive manner at an early age that will filter through and show people that it is not something to be feared but it is something which could be managed.

Q454 ***Earl of Erroll:*** I found the best education for my sons was when they got a whole lot of viruses as a result of being very careless on peer to peer networks and after "Daddy" spent some time clearing them off they started to wake up to it, and maybe you should contaminate schoolchildren's computers deliberately so they can learn how to remove them!
Mr Isbell: That can be a very hard lesson to learn and very time-consuming for the parent, as I am sure you are aware.
Mr Sunner: If I could make one comment relating to that point, I think education is certainly important and I think initiatives like Get Safe Online have been very useful at raising awareness, but we have to be realistic. The technical nature of these problems now is very, very carefully engineered and it reaches a point where the primary solution now has to be a technical one rather than education, unfortunately. I think education is useful, but treating it with individual powers is a very specialist task and the bad guys are very aware that the weakest link in all of this stuff is actually the human at the other end, and that is why social engineering is so powerful. So whilst education is definitely useful, I think the focus should be a technical one.

Q455 ***Lord Sutherland of Houndwood:*** I am sure that is a wise comment, but equally a very basic thing if you are new to the business is about what looks like a suspicious email. You do learn the more you do it, but if you are starting and you get something from Robert—well, I know dozens of Roberts, so how do I know that this is not one of the bad ones?
Mr Isbell: That is certainly where the targeted attacks are coming in. They are using that social engineering to try and get you to open up the emails and to click on the link, so to speak.
Mr Sunner: Worryingly, thanks to social networking, these emails can now be addressed to you with your actual address, possibly even referencing your siblings, depending on what you have keyed into these certain sites. That really has not happened in anger yet, it is very early days, at an embryonic stage, but that is what we are dealing with. So educating against that—it is such a moving target that the emphasis has to be on the lines in these protocols themselves, first and foremost.
Mr Isbell: Just to add to that point, there is another thought that as we get down the road of more mobile phones, multi-purpose PDAs, et cetera, then the user awareness and the user environment also has to take care of those evolving threats which are going to come with our new technology.

Q456 ***Earl of Erroll:*** Were there any instances in fact last Christmas with some of the greeting cards, particularly ones which were hosted on websites, containing anything like that? Certainly I had two that I did not go and visit because I was not certain about the organisations they came from. Were there any cases of that?
Mr Wood: That is quite a common technique, especially around holiday periods like Christmas, where you can have a high number of those types of attacks where they will use the social engineering of being able to receive a greetings card. You are not going to necessarily know who sent that or whether it is from somebody you do know. The inclination is to click on the link and that is where they transfer the attack from the email scenario over to the web and then they can use exploits on your browser to then infect your machine through a different channel.

Q457 ***Lord Mitchell:*** Just before I ask my question, just for my own knowledge, what percentage of domestic laptops or computers actually have anti-virus software on them?
Mr Isbell: That is a very good question. I do not think we have the detailed analysis.

Q458 ***Lord Mitchell:*** What would you guess?
Mr Chantzos: Globally?

Q459 ***Lord Mitchell:*** Let us just take the UK to start with.
Mr Isbell: One thing I can say is that there are 318 million customers who launch our live update every day, that is globally. Does that help give you the size?
Lord Mitchell: Well, sort of.
Chairman: There are 2 billion cell phones in the world at the moment and about 600 million PCs.

Q460 ***Lord Mitchell:*** If you had access to that information, it would be really useful to get that.
Mr Isbell: We can certainly investigate whether we can get you some detail on that. The only other statistic that I brought with me is that we currently have 120 million desktop gateway and enterprise AV systems deployed out there, so again based on market share we might be able to extrapolate some information for you.

Q461 ***Lord Mitchell:*** A question to MessageLabs, if I may. In your submission you talk about targeting trojans, which you regard as one of the most significant threats in recent years, and we really wanted to know to what extent do these affect individuals or are they largely an issue for corporate security?
Mr Sunner: I think it is first and foremost an issue for corporate security, but this is something which is at a very, very early stage. Would you mind if I took a step backwards to illustrate what we are really talking about here? This is at the other end of the scale. As opposed to something which is very high volume, these are the one-off. In January 2006 we were intercepting two instances of this behaviour per week, so that is two within one and a half billion emails, a very, very feint blip on the radar. This month, January 2007, that ratio is now one per day. So this is the Trojan which has been built with the express intention of getting inside a single company or a single individual's machine and to then allow remote access into that system. Because it is a one-off, the chances of that ever getting onto the radar of the broader security community become just about zero. The purpose behind this is to gain remote control of the machine for the purposes of taking off data or in the corporate world industrial espionage. But if that individual, perhaps, is an author or someone who has some intellectual property of some worth, he is a potential target. What is worrying is that towards the end of 2006 toolkits appeared to make these kinds of trojans. So suddenly the barrier to entry has been lowered. All you have to have now is the intention and you can buy this capability from certain nefarious Russian websites, as opposed to potentially needing a really high degree of technical capability. As we have seen with viruses back in the early 1990s with traditional viruses but without being malicious, the minute toolkits appeared, lowering the barrier to entry, a slew of viruses followed. We are at that early embryonic stage now with targeted attacks, so we would anticipate that whilst the ratio is one per day within two billion emails at the moment, I think very conservatively by towards the end of this year, by December, that ratio will be closer to between five and ten.
Mr Wood: The other concern from the targeted attack perspective also is that if your machine becomes subjected to the control of one of these criminals where they install a botnet code onto your computer which then gives them remote access, they then have access to your files on your computer. We have seen instances of spyware then appearing on those machines which then report back other information to the criminals where they really take off kind of extras on the side in terms of payment for hosting the botnet code. So if they want to send out spam emails, for example, then if they find any other information which may be of benefit to the criminals then they will use that to their advantage, and in so doing they can deploy spyware onto those machines and use that information which they gather to understand your browsing habits, which banks or which online sites you will then visit. As my colleague mentioned about the trojans which are now starting to appear, they are now becoming customised to particular banking sites where most of the phishing activity we see at the moment targets banks and organisations which do not deploy what is called the "two factor authentication" where you have a key fob, for example, which will authenticate as well as your username and password, because once you lose your username and password then anybody can then gain access to your bank account, potentially. If you have a key fob, which you physically have, then that gives you some degree of protection, but what we are now seeing from the trojan perspective is that the trojan will potentially take over your browser session after you have completed the authentication. So rather than stealing your personal username password, it will wait for you to authenticate, and if you never go to that particular site that trojan may be just dormant on your machine, and that is certainly where we are seeing some increased activity now.
Mr Isbell: In principle, we agree with MessageLabs's findings. On targeted trojans, with the social engineering the targeted nature of them makes it less likely that they will be reported and appear on the radar.

Q462 ***Earl of Erroll:*** Presumably they are using standard toolkits which they are downloading from websites, wherever? Those will have a signature to them and you will be able to recognise the code and it will make it much easier to clean them up?

Mr Sunner: First of all, the toolkits are not standard. The emergence of toolkits is quite new and kind of worryingly if you buy one of these off-the-shelf trojans you actually get the bad guy equivalent of a service contract, so that if detection for your newly-made trojan starts to appear they will send you a new version. Unfortunately, it is all too easy to keep this kind of code alive, not by changing the code but by changing the encoding format it is stored in, which will basically in effect give it a new lease of life from traditional detection methods.

Q463 ***Lord Mitchell:*** Just a couple of points. The first thing is, since they are so hard to detect do you think that is going to give individuals a false sense of security?
Mr Sunner: The first thing is the level of awareness of this. Because it is in such low numbers when compared with things like spam or phishing, I do not believe this is really on the broad radar, certainly for the consumer and even for the corporate world. I do not think people realise the potential which is out there at the moment. I think if they did, then they really ought to be focusing on putting defences in place which can stop this stuff, because frankly traditional detection methods, which are reliant on signatures, which are ultimately reactive, are blind to stopping this new kind of threat.

Q464 ***Lord Mitchell:*** In your evidence you conclude "defensive countermeasures woven into the fabric of the Internet itself will become the key component of any . . . solution." Then you describe it as "fundamentally a technical problem [which] will always require a technical solution, first and foremost". Do you see risks in placing such dependence upon technical solutions and should not end-users, whether criminals or private individuals, be the prime focus of our attention?
Mr Sunner: The Internet was fundamentally based on protocols to be opened and in some cases things like email were designed decades ago and never catered for the kind of abuse which is now taking place. So the kind of security we are talking about is a fundamental requirement which is missing, which must be there. Unfortunately, given the technical sophistication of some of these trojans which we are talking about, I think it is really out of the reach of what you solve with education now. How can you educate, for instance, against something which is a perfectly rendered online banking site to all intents and purposes? You cannot tackle that with human education, it has to be by spotting the malicious code behind the scenes, which you can only achieve with Internet-level filtering.
Mr Isbell: I think we are seeing that this is the ever-changing threat landscape which is an on-going feature of the Internet and how we have to react to the threats and new threats as they appear. Whilst I agree with my colleague about technical means, technical countermeasures to technical attacks and technical threats is a requirement, I still think that a multi-layered defence is practical to give you some defence in depth.

Q465 ***Lord Young of Graffham:*** Most of what I wanted to ask about actually has been covered, and perhaps I should say at the start that I am not bothered about marketing spam. By coincidence or otherwise, we use MessageLabs and very few actually comes in, and also Symantec on some machines, and others, but what does concern me greatly are the things you have just been saying for the last few minutes about having tailored trojan horses coming into the network. Things have got so bad that in companies which I am involved with any IP we keep on networks which have no access to the Internet for that very reason, so we get in the ridiculous situation of not being on the Net, we are on an intranet, if you like, with no connection outside. If you can see a world in which criminal forces essentially can tailor-make a trojan horse to attack a particular bank, what is that going to do to the future of banking, Internet banking, and indeed inter-commerce banking? Is it going to go off the Internet and have to go into private networks?
Mr Sunner: I think we have to bear in mind that this stuff succeeds at the moment because there is no detection in the majority of cases in the stream of traffic, so we are talking about an open target from the bad guys' perspective. This is why we believe quite passionately that we actually urgently need this level of filtering to be interwoven into the fabric of the Internet. Now, whether that is us or whether it is with other ISPs adding this to the flow of traffic, that is how this problem will get solved. So I do not think that we are heading to a situation which is unsolvable. The source of all this is the Internet, therefore that is exactly where the solution needs to be.

Q466 ***Lord Young of Graffham:*** We have had evidence in some of these sessions about whether security should be at the centre or at the periphery and there is a difference of opinion, but what you are telling us, I think, is that these are tailor-made viruses and tailor-made trojan horses attacking a specific target, and very few of them, and therefore the detection software has not been developed. How is it going to be developed in the future, because if I were doing this I would be looking at one specific trojan horse to attack one particular bank account, to remove one large amount of money and then stop? That is like trying to develop something in the medical world against an illness which only appears once.
Mr Sunner: That is absolutely right. Basically, this is where with scanning at the Internet level a lot more becomes possible in terms of the computational power which you can throw at the problem. It would really be impossible, for instance, to be decoding all potential

encoding formats on a PC or on a gateway. You just cannot do that, which is why those mechanisms are reliant upon getting signature updates. At the Internet side of things, all those things do become possible and that is how we are able to spot this stuff at the zero hour. As I say, whether that is us or whether it is another vendor, I think the sooner we can get that level of aggression into those protocols, which at the moment are currently wide open, the better and that is when this problem will start to abate.

Q467 ***Lord Young of Graffham:*** But would you detect the first occurrence?
Mr Sunner: Absolutely.

Q468 ***Lord Young of Graffham:*** You could be capable of that?
Mr Sunner: Yes.

Q469 ***Chairman:*** There is a very small chance that you will miss one of these trojans?
Mr Sunner: Correct. I would say it is incredibly small. From a malware perspective, ironically the more they try to disguise themselves, from our perspective, the bigger these things stick out. So they are generally always inside office documents and are reliant upon the heavy use of encoding formats to disguise the presence of these trojans. This is where, if you have a lot of computational power, which you have from being in the fabric of the Internet, you can get inside those encoding formats. The key thing is decoding it. Once you can do that, you can see the malware.

Q470 ***Lord Young of Graffham:*** Does this cause a backlog, does it take time, and what is it going to do to the transmission of material?
Mr Sunner: Email is a store and forward mechanism anyway. You are generally dealing in seconds, so it would not be something which would really be perceptible, but I think you also have to weigh up what we are actually doing here. The actual risk, as you have mentioned, in terms of loss of intellectual property could be absolutely devastating.
Mr Isbell: If I may, the loss of intellectual property is a higher value asset, so the strategy even for the individual user, but especially with corporate, should be to do a proper risk assessment and put in place a proper risk management strategy for its intellectual property and its high value assets.

Q471 ***Chairman:*** If you can detect them so easily, do you also know who they are?
Mr Sunner: What you can tell is the origin from an IP perspective. Internet addresses have geography, a bit like a phone number, but whilst you might be able to see the origin that is a particular region, whether that was compromised by some other region is the bit that you actually do not know. So depending on where these things are originating from—obviously people are motivated to employ a very high level of stealth and whilst you can tell the geographic origin, that does not necessarily belie the perpetrator.
Mr Chantzos: My Lord Chairman, if I may, to address the question of detection is a question of, if you like, technology as well as a question of legal instruments in the sense that the process of tracing back to the perpetrator requires first of all that you are able to capture the IP of origin, the last IP of origin, it requires you to be able to go to the service provider through which the IP of origin originated and ask to find any relevant information which that service provider has regarding the IP of origin. Maybe that information has been stored, maybe not. If indeed stealth technique has been employed, if there has been "hopping", if you like, between different geographic locations through compromised computers, then you need to be tracing back through the different geographic locations, through mutual legal assistance agreements involving the law enforcement authorities of every different country. Often, as this requires access to personal data, you would require police warrants. As a result of that, depending upon the level of co-operation between the different law enforcement authorities, which may vary depending on the country—within the European Union, for example, there are established routes and channels—it may be more or less easy to trace.

Q472 ***Lord Patel:*** I want you to take this question seriously: how many "zombies" are there in the United Kingdom?
Mr Isbell: I do not think I have that level of detail with me to answer that properly.
Mr Wood: Certainly the last time we did any research into this is going back to probably about the third quarter of the end of last year and we estimated around about 140,000, maybe slightly less, at that time in the UK, which is about 4.3 per cent of the computers which we were intercepting malware traffic around the world based in the UK. It is likely that number may be higher, although there is some evidence to suggest that over the recent holiday period over Christmas the botnet numbers actually decreased quite dramatically, probably around about 20 per cent worldwide, because a lot of people either turned their computers off for a length of time or they went out and bought new, faster PCs because maybe they thought there was a problem with their computers.

Q473 ***Lord Patel:*** How would an individual like myself know whether my computer has been taken over or not?
Mr Sunner: As you say, of course, to answer all of these questions seriously it become incredibly difficult to ultimately confirm absolutely yes or no because the level of stealth which some of these trojans can employ can actually bluff the whole operating system, let alone

the anti-virus software, into their presence so it become virtually impossible. Having said that, if your computer, if it is a single machine and you have not been doing anything on it for a very, very long time, let us say five hours, yet your activity light for your cable modem or ADSL connection is very, very busy consistently and is for a very long time that might be a clue that something is awry, not 100 per cent sure, but it might be an indication. If the machine is obviously slowing down substantially, married with that, I would certainly be suspicious.

Mr Isbell: If I could come back on that. I apologise, I did bring some information with me. From our research the UK has seven per cent of the botnets in the world during the measured period behind America and China. The UK accounted for only two per cent of all known command and control servers of those botnets, which indicates that the majority of botnetwork computers in the UK are likely controlled by servers which are outside the UK. We observed an average of 57,700 active botnetwork computers per day with over four and a half million distinct botnetwork computers which were identified as being active at any point over that six month period. I do not know if that gives you the flavour of the scale you were looking for.

Q474 ***Lord Patel:*** Yes, significant. So why do these bot-attacks originate in the UK? Why does the UK have such a high rate?

Mr Sunner: It is a global phenomenon.

Mr Isbell: It is a global phenomenon, yes, that is correct.

Q475 ***Lord Patel:*** So the UK is no worse than any other?

Mr Sunner: The UK is in no way particularly singled out.

Q476 ***Lord Patel:*** So what is the Government doing about it?

Mr Sunner: From a traffic perspective, the ISPs will be closest to this and they are, of course, self-regulating so I think the Government is a stage removed from this problem currently.

Mr Chantzos: When we are looking at it from a public policy standpoint obviously, as we said, information security is an issue of people, process and technology, and regulation is by no means the only solution but regulation is certainly an aspect in this area. So to start with, as I am sure you may be aware, the Computer Misuse Act has recently passed also through this House. The Computer Misuse Act was recently updated to include things like denial of service attacks as part of its criminal aspects. It was also updated to include an offence similar to what is called the misuse of device, in other words using it as a hacking tool, and now it is at the stage of implementation. The updating of the Computer Misuse Act is a positive step. Nevertheless, we as a company and my understanding is that a number of other technology companies in this area feel that it is important there is adequate clarity about the issues which the Computer Misuse Act is covering because the current language is to an extent open to some diverging interpretations and it is important that it is clear about what aspects which the Home Office and the Crown Prosecution Service want to see criminalised. One aspect is that right now from a regulatory standpoint there is also a debate in Brussels about what can be done in the area of information security at the European Union level. The Commission has put some proposals around the review of the directive 2258, which is covering the protection of individual privacy on electronic communications. Some of these proposals open a discussion about a more active role of the ISPs in the area of information security. Some of these proposals also pose the question of whether there should be a similar regime to that of the US in the area of breach notification. I think also if one looks at the directive 9546 and how that has been implemented in the UK regarding the Information Commissioner, both 2258 and 9546 cover the question of the issue of data protection and information security, so we believe that the Information Commissioner perhaps could see more powers in this area, to be more effectively able to investigate and follow up cases relating to these kind of abuses, spam certainly being an aspect of it. Also, there is the Council of Europe Convention on Cyber Crime, which the UK has signed but has yet to ratify. The United States have recently ratified it and a number of other countries at the Council of Europe have ratified it. The Council of Europe Convention is by far the most complete international instrument in terms of law when addressing cyber crime.

The Committee suspended from 4.22 pm to 4.30 pm for a Division in the House

Q477 ***Lord Patel:*** How big are these botnets and what are they used for?

Mr Isbell: I think they vary in size in terms of the botnets themselves in discrete networks owned by a command and control service, so they vary depending on how many clients they have actually managed to infect. Obviously the object of the exercise for every bot-master is to increase his networks to the maximum possible because that makes him more attractive in a financial sense when he is actually selling that capability on. It is a progressive thing. Botnets will grow and they grow depending on how active that particular bot-master is.

Q478 ***Lord Patel:*** What are they used for?

Mr Isbell: We are seeing more and more increases, moving away now from the traditional area where somebody wanted to be famous. It is now more

financially-driven, for financial gain. It is money and it is more around the retail markets as well as getting identity theft, and those two seem to be the main areas of focus.

Q479 ***Lord Patel:*** What is the biggest one that you know of?
Mr Isbell: I do not think I actually know the biggest botnet itself. I can come back to you with that particular piece of information.
Mr Chantzos: I am aware of cases which have been publicised that law enforcement authorities have come up with, botnets which had even a million IPs. To come back to your question, the motto we use to describe this sort of activity is that hacking is no longer for fame but for fortune!

Q480 ***Lord Sutherland of Houndwood:*** It seems to me that we have moved beyond crime into warfare, and if that is so are these sites vulnerable to attack—to make it not worth their while, in other words, because you keep destroying their capacity? Do you say the solutions are technical the other way round?
Mr Isbell: As a vendor we do not actually go on the attack, we are in the protection business.

Q481 ***Lord Sutherland of Houndwood:*** Sure, but that was not my question. My question was, could they be attacked?
Mr Isbell: Yes, they could, is the quick and short answer, from information that is found, but that would then be up to law enforcement because attacking itself can be deemed as a criminal offence.
Mr Chantzos: Also, when you are looking at dealing with these kinds of networks a key point is taking out the command and control centre because if the command and control centre is, let us say, in some Eastern European country, it can within a few hours reappear somewhere else. So it is very important that when, if you like, you cut the head of the snake you cut it for real and then burn it and incapacitate the rest of the body.
Mr Isbell: We have certainly been involved in assisting to close down networks, especially the anti-phishing type networks and using the co-operation to assist in providing information to help law enforcement agencies actually do that.

Q482 ***Earl of Erroll:*** Just on that last question, surely the problem is that the moment you start attacking a "zombie" on someone's computer without permission you are altering the contents of their computer and you might do that inadvertently and destroy some of their data? So it is not something, surely, you can do from outside? Would you agree with that?
Mr Chantzos: My understanding is that the existing legal framework does not actually allow that as a defensive mechanism you go into a counter-attack. My understanding also is that the role that we see for ourselves is not to police the Internet but to protect our clients. The role of policing would for the law enforcement authorities, who would have both the power as well as the means to do that policing.

Q483 ***Earl of Erroll:*** I would like to get on to that in a second, but just before I do, is part of the problem that the virus checkers that you deploy or have been deploying over the last two years are basically perimeter security, in other words they check things coming in through the perimeter of the computer, whereas once it is inside it can get on and do what it likes? So in order to check that my computer has not been infected, I have to have other software sitting there, for instance Spy Watch, Search and Destroy and Adaware and things like that, checking for internal problems, because your software only deals with stuff as it comes in through the perimeter?
Mr Isbell: No, absolutely not. The software that we deploy does protect at the perimeter but also protects in depth at the centre of servers, et cetera, so it is a multi-layered defence approach.

Q484 ***Earl of Erroll:*** But on my laptop, if I have your software it is not checking for trojans inside the whole time?
Mr Isbell: You can run full scans, et cetera. Is that what you are looking for? I am sorry, I am not fully understanding your question.

Q485 ***Earl of Erroll:*** It is not continually checking against odd, aberrant behaviour inside the laptop?
Mr Isbell: Yes, it is, but it is checking definitive actions which the computer is actually taking, opening files and so on. If you are looking for the answer about checking anomalous behaviour, there are some heuristics built within the software that we provide but it is not detailed or complex.
Mr Chantzos: In addition to that, there is the question of controlling the outbound traffic which is taking place also in terms of the software solutions we provide, but also if one was to look at other even more high-end technological solutions available in the market there is, for example, the capability of real-time monitoring security devices whereby by doing that you are in a position to detect anomalous behaviour either inbound or outbound, in which case you are able to detect even unknown pieces of code, malicious code, which you have not been able to see before and therefore stop it from going outside. It is part of, if you like, collection of information, analysis, correlation and response. It is an element of predictive defence.
Mr Isbell: It is important that the software is kept fully up to date with the latest known attacks and most of the software which is deployed nowadays contains two or three parts. There is the anti-virus, there is the firewall and there are the entry detection systems.

Mr Chantzos: Forgive me, but if I may jump into this one more time, my Lord Chairman, there is also a regulatory aspect to it, if you like, in the sense that if one was to look, for example, at the eCommerce directive right now as it currently stands, the 2001 directive, which is part of UK law, my understanding is that the directive does not require prior monitoring of their eCommerce to provide infrastructure as part of its security technology. There is an explicit requirement of no prior monitoring. As a result of that, in the current trend landscape that we have just discussed with, for example, targeted trojans perhaps that may be an issue which I think Brussels needs to revisit.

Q486 ***Earl of Erroll:*** That brings me on to really the point I want to raise, which is are the UK laws on spam viruses adequate and appropriate at the moment, or where would you see a need to change them?
Mr Chantzos: In my effort to answer the previous question from Lord Sutherland I tried to lay out as succinctly as I could the regulatory framework, which is rather complex. In a nutshell, we think that the Information Commissioner could be doing more in this area but would need to be empowered adequately in order to be able to do that.

Q487 ***Earl of Erroll:*** You remind me, that was one of the things I wanted to ask you. Why have you set up yet another body doing that when we already have the police site trying to do that and there are others at the policing and enforcement end with powers of arrest and things like that trying to work on this. Surely it would be more sensible to reinforce them than to have yet another person who is going to have to acquire investigative powers?
Mr Chantzos: To start with, I am not suggesting that we should establish a body. The Information Commissioner, as I am sure you know, is already there. Having said that, having the Information Commissioner, having more powers in the area of dealing with issues relating to information security—in fact the European directives foresee a role in this area—I do not see that being unreasonable. Of course, ultimately the arresting powers and investigative powers around this should be the police. The UK police, I believe, are doing a rather good job in this area, but they can always do better. There can always be more resources. There is also a challenge which has to do with the reporting of the eCrime, that is to say whether eCrime is actually being reported as eCrime or whether eCrime is actually being reported as fraud, for example. We had this discussion internally and, quite frankly, maybe it merits a wider discussion, whether there should be a central depository for depositing eCrime or whether that can be done at a regional level. All these are elements which one could further review to try and see where there can be improvements in the system, but to start with when it comes to legislation, to things which could be changed, as I said the issue of breach identification, which is currently under discussion in Brussels and is already under discussion in the US, perhaps that is a step in the right direction. As I said also, in Brussels right now there is discussion about the role of the ISPs and in the UK the Computer Misuse Act has been updated to address these issues. We would like more clarity around what is in the Computer Misuse Act, but in principle that is a good step. Giving more tools to the law enforcement authorities to do their job effectively would certainly be something we would welcome. So, if you like, the UK is going in the right direction. The question is, perhaps, going the extra mile and co-ordinating that with the other international figures and the people whom the UK is teaming with.

Q488 ***Earl of Erroll:*** Is part of the problem—it is this cross-border, global aspect to it—that there are people in the UK who should be prosecuted and cannot be? Is that part of the problem?
Mr Chantzos: That is a very good question. Are there people who should be prosecuted in the UK? My understanding is that in the past there have been cases whereby people were not able to be prosecuted or were able to get away relatively lightly on offences. Having said that, as I said, the fundamental instrument around this area, the Computer Misuse Act, has been updated to address this issue. We would like the Computer Misuse Act to be more clear. However, we need to see information security as a dual approach, so there is the prevention side and there is the detection and prosecution side. The Computer Misuse Act and the data retention legislation, which would give a possibility that you can trace back via the ISPs, is dealing with the suppression and prosecution side of things. If one was to look at the prevention side of things, for example establishing a breach notification regime, as we have seen in places like the US, it could function as a great enabler of information security because it creates incentives for people to invest around this kind of technology. It is a question also of facilitating, promoting, motivating people to go down this path rather than just merely mandating the suppression of the offences.

Q489 ***Earl of Erroll:*** So you see the Information Commissioner as being on the preventative side rather than the resource side?
Mr Chantzos: Yes. I am sorry if I did not make that clear.

Q490 ***Lord Sutherland of Houndwood:*** You have been eloquent in saying you think the police are doing quite a good job, which is very reassuring to hear you say that. Do you have any system for sharing information, because a lot of the information which has come out

today I would have thought would be of great interest to those concerned with law enforcement. Is there any systematic way this is done? I ask both companies to respond on that.
Mr Chantzos: Obviously the law enforcement authorities as well as anybody else who is willing to acquire by normal commercial means have access to the Symantec intelligence network and early warning capabilities. That is the first aspect. As a general rule, I would say that Symantec is a good corporate citizen and a responsible one, so when requested by the law enforcement authorities via the appropriate channels and within the boundaries of the law, we will respond to a request.

Q491 ***Lord Sutherland of Houndwood:*** But that means in effect the boot is on their foot, they must take the initiative on this, rather than a sharing of information?
Mr Chantzos: If you look also at the way the criminal and justice system works, there are rules of secrecy around the way the investigation is taking place. We cannot, and we should not know what it is the police are investigating. They should reach out to us and tell us, again provided they do that via the proper channels and appropriate means. Quite frankly, there is also the question, do we have it to give to them? Sometimes it could be that it sits on the desktop of the individual in question.

Q492 ***Lord Sutherland of Houndwood:*** Clearly there are two different sorts of information. One concerns a specific inquiry and what you say is absolutely right there, you cannot have prior knowledge of where the police are going, but there is also the more general point, the kind of information you have presented this afternoon, both of you, about trends, the way in which things are developing?
Mr Chantzos: The data, for example, that Mr Isbell presented to you today regarding the Internet security threat report. These are, I would say, publicly available for free and I am sure that the law enforcement authorities are able to tap into them, if you like. In addition to that, I am sure that there would be also contacts and the possibility to ask a question about Symantec, "We read this. What does this mean in your report? Where do you see the future going?" So I think that they have the resources to tap into should they want to do that.
Mr Sunner: I want to give some positive feedback here. We have always enjoyed a very good relationship with law enforcement, formerly the National Hi-Tech Crime Unit, now SOCA, and what we find is, as I think has already come up, when a threat is taking place you will find that the marketing people, be they the ISP, the mid-carrier or the end point, will have a bit of information. So from our perspective in virus terms if we make an interception—because a lot of the viruses we intercept are viruses which are broken, which do not actually work, so the person on the end who is actually creating this is there. If they are not very smart, when they sense that it is broken they try and fix it, so what we sometimes see is the seeding, the deliberate seeding, and if it is all coming from a single source that is a very, very important piece of information. What we know is just the source IP address. That will be from an ISP that we are probably not connected to, but at that point we give that information to law enforcement. They then will approach the ISP and hopefully might be able to unlock that next stage and that kind of relationship has worked very successfully in the past and I think it is one of these things which will become better as cross-relations between ISPs, as we are sharing the back-channel traffic about what came from where, become more open.

Q493 ***Lord Sutherland of Houndwood:*** Is there any link with the police in terms of providing support for training, and so on, in this highly specialised world?
Mr Isbell: We do run specialist courses and obviously the police can avail themselves of those and we do provide them when requested.

Q494 ***Lord Sutherland of Houndwood:*** But it is again when requested?
Mr Isbell: Yes.

Q495 ***Lord Sutherland of Houndwood:*** Does that apply to MessageLabs also?
Mr Wood: Certainly in my experience we have got a very skilled team of engineers who work very closely with the new emerging threats and when they discover something new they are in a position where they have the knowledge to be able to understand what is going on and understand how it works very quickly. They have very good relationships with the enforcement authorities and exchange information both ways. It is a two-way flow of information, so it is not always just about, "This is where we first saw something," it is also maybe about how it works, maybe other areas where they can look where we cannot, things that we cannot do that they have more authority to do.
Mr Sunner: Quite often some of the intelligence we might have actually might be about stuff which is not in this country and that becomes harder for us. So we have again enjoyed a good relationship where we pass that to law enforcement, who maybe do have better, smoother contacts to another region to track something down, and again that has been quite successful. So I think the relationship is good from our perspective.

Q496 ***Lord Sutherland of Houndwood:*** I find this reassuring because clearly it is a very highly technical specialist area. Just one slight change of tack, finally. We have a Government which is very keen on targets.

Do you think it would be good to set some targets for the police in this area? Would that jolly things up a bit?
Mr Chantzos: In the private sector we also tend to talk about targets, objectives, key performance indicators. One of the key questions, however, before we set an objective and agree to it—and I am saying it as a manager myself, I have to go through the process with my members of staff—is the question of is that target achievable? The second is, is it adequately resourced for it to be achievable? So before we look into the question of is it adequately resourced, I think it would be unfair to look into the question of what the target should be.

Q497 ***Lord Sutherland of Houndwood:*** I think you could give a seminar in this Palace of Westminster. It would be very helpful! Do you think, nonetheless, the setting of targets, if sensibly designed, would actually move things on?
Mr Sunner: Speaking personally, I think that what we are dealing with is such a moving target that it would potentially become difficult. We have seen the threat profile change dramatically in terms of viruses, spam, phishing and spyware across the board in the last six months, so if we were to try to articulate the things we were looking for and the threat profile six months ago, things have occurred since then that have changed the landscape. Therefore, I think it would be very, very difficult to set targets that flow all the way down to law enforcement that could be policed. I just do not think it would be viable.
Lord Sutherland of Houndwood: That is very interesting. Thank you.

Q498 ***Lord Mitchell:*** This is for Symantec really. You claim "a competitive market for [the] security software industry protects diversity and thereby enhances security". Do we have a competitive market at present, or should we be taking steps to improve things, and could you not just refer to the UK? This is a global market so I just wondered if you could do it from that point of view also?
Mr Chantzos: Absolutely. Where do you start? To start with, you have MessageLabs and us, but obviously there are more than ourselves. Right now we believe we have a very competitive market and we think that this is the way to go. We always prefer that we let the market operate and the market forces work at their will. Obviously, there is a role for government to play and there is a role for the competition authorities to ensure that there is a level playing field in this area. It is difficult for just one company to deal with the complete Internet security issues as they emerge and as they form, therefore competition is necessary in order to create the level of innovation and the level of technology which would react quickly and efficiently to the new security threats. Having multiple providers means that the market can deal with the specific attack, the specific threats and the different players who are experts in their area can then, if you like, identify and address these threats in their niche market. That effectively ensures a wider net of response. Finally, having a monoculture of information security is risking to create a single point of failure, so should this single point of failure for some reason fail, should this single security posture fail, it has the risk of having a knock-out effect for the rest of the infrastructure, which is why it is important to have diversity in the system. It is very much a biological example, if you like.

Q499 ***Lord Mitchell:*** At one of our previous sessions on 17 January Microsoft was here, Matt Lambert, and he was asked about the company's dispute with the European Commission over anti-competitive behaviour, particularly with respect to the new Vista operating system, and he defended Microsoft's position and claim to that, and again I quote: "We have always worked with other companies, including competitors, to try to make our systems as inter-operable as possible." I would like your views on that, please.
Mr Chantzos: Your question is about inter-operability, if you like?

Q500 ***Lord Mitchell:*** Is it a competitive market, or do people co-operate, more to the point?
Mr Chantzos: We have enjoyed a longstanding co-operation relationship with Microsoft. We believe it is important that this co-operation relationship continues exactly because ultimately it is also better for the users. It is better that we work together to protect them, as opposed to working in different directions. At the same time, this must not be done at the expense of inter-operability. Ensuring an adequate level of inter-operability ensures diversity in the security system, it ensures that customers have freedom of choice, freedom to choose what security solutions they need for their own security posture, for their own security needs. It also ensures that the consumer, the average user is not biased, is not dragged into a particular security technology which perhaps may not be his choice. It ensures that there is innovation and ultimately ensures that we avoid having a single point of failure. To go back to your question, yes, I maintain the point that we have a very competitive marketplace, but I also maintain the point that it is the role of the industry and the competition authorities to work together to ensure that that level playing field remains.

Q501 ***Lord Mitchell:*** And as for software security being built into the operating system?
Mr Chantzos: Having baseline security is obviously better than having no security at all. At the same time, the security of the operating system is not necessarily a security solution and taking some steps to, if you like,

harden the operating system is a step in the right direction. However, the challenge we have on baseline security is first of all the evolving threat landscape. The fact that it is baseline means that it is basic. The threat landscape is such that, quite frankly, the type of threat which most users are facing is far higher than what the baseline security is providing and also having a baseline security, unless the user is adequately educated, runs the risk of providing a false sense of security.

Q502 ***Lord Patel:*** Symantec suggests that "diversity in software platforms and applications is key to containing the spread of security threats," so who is going to be responsible for achieving this and how?
Mr Chantzos: Do I understand your question correctly as asking me who is responsible for entering the security?

Q503 ***Lord Patel:*** No, it is based on Symantec's quote that "diversity in software platforms and applications is key to containing the spread of security threats". So how are we going to achieve this diversity in software then?
Mr Chantzos: It is not our job to dictate changes in products or the choice of consumer, clearly.

Q504 ***Lord Patel:*** Whose job is it?
Mr Chantzos: Certainly not ours. However, we do think it is important that we work together, that we work in an inter-operable environment to deal with security threats.

Q505 ***Lord Patel:*** Let me be more challenging. We know Microsoft controls most of it. Microsoft will argue that those who want to attack it are going to attack it for money, so having diversity does not solve the issue?
Mr Chantzos: I am sorry, but you need to see it not from the perspective of, "I want to attack for the money," but from the perspective of threat, vulnerability and risk management. If you see it from that perspective, I am attacking something which is vulnerable, which is widely deployed, and I hope to be able to exploit it so as to be able to capitalise on all of that. So to go back to my original point, having diversity in the eco system and having diversity in the security solutions which are there means there is no single point of failure which, if exploited, would be able to take out the entire infrastructure successfully. As I said, we have been working together with Microsoft and we hope that we will continue to be able to work together with Microsoft. At the same time, the choice of the technologies and the choice of the security around the technologies should be left to the user and I would like to stick with that, if you like.

Mr Sunner: It is a really good point and I think the reality is we do have a dominant eco system in terms of platform, which is Windows. I think it is really interesting to note that now that the iPod generation is entering into the workforce and Macs and OSX is right back in vogue, sure enough the volume of vulnerabilities and things being discussed for Macintosh is going up. The only reason for that is because it is becoming a viable eco system in its own right. In the same way one of them will have attacks or threats inside email and web and instant messaging, because they are ubiquitous eco systems whereas currently the iron world is silo'd. So I think eco systems will always appear. It is desirable to have diversity, but by the very nature of us as users driving common platforms the eco systems will appear and then they will be attacked. So I think it is nice to have diversity, but the reality is that things will always gravitate towards a single platform, as we have seen with mail platforms, web browsers, et cetera, and then the threat will unfortunately follow.

Q506 ***Chairman:*** Would we not be better with a single operating system but a diversity of security systems to protect it? At least you know what you are protecting. I would have thought multiple operating systems is going to dilute the security software world?
Mr Sunner: Actually it makes it a lot more complex and possibly even unattractive for the attacker if you have diversity because if you have got a smaller eco system it may not be attractive to attack, but the reality is that you will end up with common platforms. That is what we as users will ultimately demand. Ultimately platforms will remain the same. I am sorry, could you just repeat the original question? I beg your pardon.

Q507 ***Chairman:*** I am just arguing that if you have got a single operating system to protect, as it were, or to make sure it is secure then it might clearly be beneficial to have that as a sort of open software task so that the world's brains could concentrate on protecting a single system. If you have two or three basic operating systems then that workforce is spread over three systems?
Mr Sunner: I think the reality is that a secure operating system is a Utopian view.

Q508 ***Chairman:*** There is no such thing?
Mr Sunner: It is not realistic, because what you have to remember is that whilst you can architect something now which might be bullet-proof today, the bad guys will not stand still. That is why we see platforms targeted in the way they are, directly proportionate to the eco systems which exist. The minute you have a platform which is dominant in any way it is a desirable target and then people will work until they do find an exploit.

Mr Chantzos: My Lord Chairman, to start with I would like to reverse the question you have just put, so have one single operating system and many security providers. Why would we not want to show innovation at the level of the operating system to start with and have just one player and not have the possibility to have many to operate with each other and many security providers as well? So why would we not want to see more innovation in this area? Why would we want to restrict innovation just to that? That is perhaps something worth debating. The fact remains that the points which my colleague from MessageLabs makes are rather accurate. The more you see a dominant platform emerging, it is normal that that dominant platform will be receiving a high proportion of the attacks, which is why both variability as well as inter-operability become key elements.

Q509 ***Lord Young of Graffham:*** Despite the best efforts of both MessageLabs and Symantec, I do get the occasional bit of spam trying to sell me another desktop protection system! I am sure it is inadvertence on your part, but there is a whole variety of systems, some of which in financial terms are fairly expensive and some of which are free. Some do it with a great deal of fuss, others operate behind the scenes much more and just occasionally send you a reassuring message. I personally operate from different machines probably three different systems. How do I tell the difference between them and how do I know, in the absence of getting an attack of some sort, an obvious attack, that they are any good? Is there any way of measuring them or actually understanding why I should pay more for Symantec rather than take a free one from someone else?
Mr Isbell: I think you have to look at the infrastructure behind it and the company which is actually putting that particular software out there which is protecting it. The larger the infrastructure, the larger the intelligence network, the bigger the set of analysts, the more sensors that are out there, then the better able we are to protect you. Therefore, having a global intelligence network such as Symantec will give you a better sense and a better view that the level of protection you are going to get is a lot higher. The danger about the free security software which we have seen is that it is the wrong way, and there is a particular case in point, one of which came through on an adware which actually was used to turn round on itself to actually get you to buy a particular piece of security software. Having a trusted partner in the security vendor with the adequate size infrastructure which is supporting it and providing the intelligence at the back end I think is one of the ways.

Q510 ***Lord Young of Graffham:*** Are there circumstances in which you would be prepared to back your trust with a guarantee, in other words, compensate customers if malware got through in some sort or other?
Mr Isbell: The problem with giving guarantees is that you have to set a guarantee up against a set of criteria. Configuration of the software is ultimately down to the user for his own particular profile and his own level of risk and how vulnerable he feels he is, et cetera. So it is hard to give any form of guarantee when you do not have control over that.

Q511 ***Lord Young of Graffham:*** Or compensation? You cannot guarantee against any event happening, but if I pay a lot more for a highly protective type of system (so I am being told) am I entitled to complain when something gets through and get compensation? That is what I am really getting at because for the consumer it is the difference, perhaps, between the expensive and the free, or not expensive but those who charge?
Mr Isbell: Again you hit the problem where if you are entitled to compensation because we let something through on our global intelligence network we would have to turn round and say, "Well, did you do a live update? Do you have the latest security software on your system that we are protecting you against?"

Q512 ***Lord Young of Graffham:*** Yes, but assuming that is the case, because all your systems update automatically as soon as you get onto the Net.
Mr Isbell: That is user-configurable about whether he wanted a live update automatically or actually selects when he wants to update.
Chairman: We are very pleased to hear that!
Lord Young of Graffham: I will not say it was the obvious conclusion.

Q513 ***Lord Young of Graffham:*** Could I ask a quick supplementary, which is that if you have a large market share suffering from the Microsoft problem does it then become of interest to the virus writers to specifically write stuff which will get around your anti-virus software because that way they know they will infect a reasonable proportion of computers?
Mr Isbell: It is true that we do see particular elements of code which are trying to get around vendors' security. That is true, but by having the infrastructure and the sensor network and the analysts which we do we are providing a high degree of protection.
Mr Sunner: If I could just take that and the previous point. I am going to be a bit contentious here. In terms of new things appearing, this is where there is a big difference between a product and a service, because ultimately how does a desktop anti-virus vendor know that there is a new virus out there which they could not catch? It is because somebody got it, somebody took

the bullet. That then starts the race against time to get a sample of that, to generate the code to be able to stop that, to make that code available and get their diligent customer to apply it. All that takes a window of time. Coming on to can people exploit desktop products, absolutely, and again here is the flaw: as the bad guy, I can download all of the currently available desktop anti-virus products, have their latest signatures in front of me and keep changing my viruses on my workbench until it sails through all of them. I absolutely know now that this will succeed because they are products. As a service, you cannot do that. You cannot take a service on a CD and try it out. You get one shot at getting something through and if it has failed you have already learnt from it. I think that is the big difference.

Mr Isbell: I think we also need to clarify the global intelligence network is also provided on a service type basis. Let me just give you some statistics, if I may, about the intelligence network which Symantec has out there. It is a vendor-neutral intelligence network. There are 40,000 sensors deployed in 180 countries. We have 6,200 managed security devices deployed. There are 120 million desktop gateway and enterprise AV systems out there. We deploy 2 million decoy accounts for spam and anti-phishing. As I have already said, we have 30 per cent of the world's email traffic flowing through our botmail system. We have four security operation centres around the world supporting 500 companies worldwide and one in the UK. As I said, we have 1800 analysts, and so on. So if you look at that infrastructure and the size of that, that is providing a service to the people who buy the AV products, et cetera, which we sell to provide that service, to constantly update them through the live update system to the latest threat landscape.

Q514 ***Earl of Erroll:*** I just want to clarify a couple of points. Can you describe how spyware works and how much of a problem is that?

Mr Sunner: The first point I would like to make about spyware is that in threat terms it is quite embryonic. The virus world will be 21 years old, arguably, this year. Spyware, conversely, as it is talked about is about five years old, so there is an issue with clarification here because in those 21 years of malware people understand what the difference is between a trojan, a worm and a virus, et cetera, whereas when people say "spyware" they can mean different things. In the early stages spyware was really about this pop-up ad-type box, something which would get into your browser so that potentially if you were searching for, let us say, "car" maybe ads would start to appear. This is about four or five years ago. In so doing, the bad guy community kind of got back more data than it bargained for. It was understanding what we were searching for, and that information has real currency. So from there these browser patching mechanisms started to be more interested in actually tracking user browsers, what we are keying in, and potentially even profiling people. Today, at the very, very sharp end of this now we are seeing root kit level stealth which is equivalent to what we are seeing in what we might call the traditional virus world. What is important about that is that traditional viruses took 21 years to go from the early benign floppy disk stuff to today, where it is all about commercial gain. Spyware has been through that same loop in five years and I think that has caught some areas of the security community slightly off-guard. Of course, the common denominator in the middle is the Internet. The Internet has always been there and is basically fuelling what is possible with spyware, which is again commercial gain, industrial espionage, all these things. Does that help in terms of clarification of where we are?

Q515 ***Earl of Erroll:*** Symantec sets a list of best practice for users, "Be aware of the difference between adware and spyware," but actually how are users expected to know the difference?

Mr Isbell: We tend to use the term now "security risks" to cover the adware, the spyware, and so on, but most of them have the similar characteristics: they are sitting there, they are gathering information and then passing that information back, whether it be tracking your consumer-type spending on the Internet or whether it is to do key logging-type activity. So we now refer to it as a security risk and try and deal with it that way.

Q516 ***Earl of Erroll:*** If I am on a website where I buy things normally, I will probably be very happy that they track my profile because they can help me go to the bits of the website I want. So that is not malicious at all, whereas spyware might be giving some other details that I did not want.

Mr Isbell: But that would be a voluntary choice because you have selected that and nine times out of 10 when you are on those websites "Do you want to receive mail?" you click the box, and also you fill in questionnaires to give information about your spending-type habits, your demographic. The spyware-type activity is more to which websites you are browsing, key loggers against your online banking to find out a little information about that.

Q517 ***Earl of Erroll:*** So does the law distinguish between the two, and is spyware legal?

Mr Chantzos: I will need to check specifically for UK law, for English law. My understanding is that the 2258 eCommunications Data Protection Directive, which should be by now part of UK law, English law, does actually forbid spyware. It goes down the path of forbidding in fact what I would describe as malicious cookies as well as spyware. Quite frankly, whether their definitions of 2258 could use some refinement we are debating with the Commission and, as I mentioned

before, 2258 is up for review and once it goes through the democratic process we will be able to see what it will look like when the process is completed. I believe that we might see also changes there.
Mr Sunner: If I could just add, again because spyware is quite an embryonic term it has yet to have real clarification. Many people will consider some of these tracking mechanisms which profile where you have been around this site and we are talking grade and risk kind of stuff. Some people consider that as spyware, whereas the people who are putting it there will say, "We are putting it there for legitimate reasons because we want to profile our activity." So there is a real grey area which exists in this embryonic term at the moment and it is not black and white where you could say that all spyware is potentially malware.
Mr Isbell: I would like to clarify that as well, because if you think, "I want to track my children's web activity," that could be deemed spyware.

Q518 ***Lord Young of Graffham:*** Is it illegal, spyware?
Mr Sunner: Again, because it is a bit of a grey area, it is covering such a broad range of things, some of which are definitely malicious code, for sure, but another spectrum which might be termed as spyware at the moment because it is quite new could be considered as a commercial tracking application. So, unfortunately, the word "spyware" is too broad a spectrum to pigeon-hole.

Q519 ***Lord Young of Graffham:*** Should there be tighter definitions?
Mr Chantzos: There have been efforts within the industry to try to find an agreed definition of what we would define as spyware, different people using different means to determine what spyware is. Some are using threat matrix, for example, and others are using complete definitions. We could certainly benefit from more clarity and that is why I say when one looks at the regulatory side, yes, perhaps these definitions need to be revisited.

Q520 ***Earl of Erroll:*** But even if you can define it, of course, you have got the problem that you can go onto some websites which appear to be spyware removal tools and actually you download something. For instance—and I hope I get them the right way around—Lavasoft's adware will help you. If you go to adware you will download something which is very difficult to get rid of and download some other stuff.
Mr Chantzos: If we were to look at it from a purely regulatory standpoint, again when you download a piece of software and you double click on the end-user licence agreement, the end-user licence agreement in its endless 5,000 word document could in fact say in there that "You are accepting by installing this software that we will be taking all your personal data, using your machine for the purposes that we have specified," and you will simply not read it, click "Next," "Next," "Next," and install the software because this is what you want. You have downloaded the software because you want to install it and the owner, perhaps, of the software would claim that it has done that with your consent and this is informed consent. This is why, for example, in the US there has been a debate around the question of having a Good Samaritan clause (as we call it), which would basically say that the security provider, for removing what we have defined as spyware (or at least we are asking the permission of the user to remove what we define as spyware), is not incurring liability for doing that because by removing software which I believe to be spyware I am faced with the challenge of then the spyware owner or the alleged spyware owners turning around and saying, "Hang on a minute, the user said that could be installed," but actually the user never had an idea about it and did not know.

Q521 ***Chairman:*** So your answer is, no?
Mr Chantzos: The answer is, no.

Q522 ***Earl of Erroll:*** There is one question I wish I had slipped in earlier when you talked about eco systems, which is, are you also now working on—and this came out of MessageLabs's answer—on things to deal with what has now being called "SPIT" and "SPASMS" and others, voice over IP and spam over SMS. Are you working on those now?
Mr Sunner: There is "SPIM", spam over instant messaging, which is our current focus, and again we actually use eco systems to very much drive our road map. So right now we see email and web are obviously very dominant forces in the corporate world as tools. IM is close runner, whereas voice over IP at the moment from the desktop perspective does not have quite the same uptake as email, web or IMAXs, therefore the level of threats also are not there yet, but as it starts to become ubiquitous the threats will appear and that is absolutely where we will focus.

Q523 ***Chairman:*** Let me ask the last question. We have almost run out of time. One security company, Sophos, warned this month that the criminals are increasingly turning their attention from email-based viruses to websites hosting malicious code. Do you agree with this, first of all, and if a legitimate website is "hacked" and as a result visitors get infected with malware, should the website owner be held responsible?
Mr Wood: I think certainly it is fair to say that that trend is definitely a pattern. We have seen increased profiling in terms of the number of attacks moving away from large email outbreaks to smaller, more distinct outbreaks which then will transfer the attack sector over to, say, a web mechanism using the browser exploit. You also mentioned earlier about the rogue

anti-spyware packages, for example, and it is very difficult for consumers to know what that actually is, whether it is a legitimate application which they should install, is it free, for example, and those can be installed on your machine just by visiting a legitimate website. For example, last week My Space came under attack where they were hosting a banner for a particular well-known rogue anti-spyware application, which if you installed it would install some components which it would in turn then flag up as being critical and should be removed, but you would have to pay money to remove that. But they were not necessarily hosting it directly, they were just selling the space to an advertising agency, who were then selling that space on to another company. So it depends on where you draw the line in terms of who is responsible and should they have taken more responsibility in understanding which adverts were appearing on their site, or should the ad agency have taken that responsibility? It is very difficult.

Q524 ***Chairman:*** So like an awful lot of this, there are no simple answers anywhere here. The situation is clearly highly complex and one can try and one can make certain progress, but there are still going to be (not a pun) worm holes through the system all over the place?

Mr Chantzos: Absolutely, my Lord Chairman.

Chairman: You have made a lot of progress and perhaps the most important thing is to educate people so that at least they can take the precautions they can and then get the aid they can as well to help them. Thank you for your time. It has been a very useful, interesting session. If you have anything which occurs to you after this session, please write to us and let us know. Thank you very much.

Supplementary letter from Symantec

May I begin by offering my appreciation for the opportunity to provide oral evidence to the House of Lords Science and Technology Committee on 31 January. At this hearing Symantec were asked to estimate the percentage of computers worldwide, and in the UK, that currently have security software installed. While we were unable to provide figures to the Committee at that time Symantec have investigated this issue internally and can now provide the following supplementary information to the Committee.

In January 2006 Symantec commissioned Tickbox.net to conduct a study of 3071 UK adults on their use of Internet safety features and/or security technologies on home computers. Included in the survey were all the security software products being used from various suppliers and vendors on respondents' computers.

As you can see from the figures, anti-virus software (90.2 percent) and firewall protection (80.7 percent) appear to be the most commonly used security technology being relied upon to protect personal computers in the UK. The low percentage (3.4 percent) of consumers that are simply relying on pre-installed, baseline security features is encouraging. As it seems to suggest that individuals are becoming more aware of the importance of having additional security features and technologies in place that are appropriate and necessary to protect their online activities.

Do you use any of the following Internet safety features and / or security technologies on your home PC?	
Antivirus software	90.2%
Firewall	80.7%
Passwords	71.1%
Anti-spyware	68.4%
Anti-Spam	61.7%
Backup Software	32.9%
Parental Controls	14.2%
I do not know ı it was pre-installed when I brought it	3.4%
No I do not know	1.1%

Research by Tickbox.net, commissioned by Symantec in January 2006

I hope this information is helpful to the Committee's ongoing inquiry. If you would like any further information, or Symantec can be of any more assistance to the Committee, please do not hesitate to contact me.

February 2007

WEDNESDAY 21 FEBRUARY 2007

Present	Broers, L (Chairman)	O'Neill of Clackmannan, L
	Erroll, E	Patel, L
	Harris of Haringey, L	Paul, L
	Howie of Troon, L	Young of Graffham, L
	Mitchell, L	

Examination of Witness

Witness: MR BRUCE SCHNEIER, examined.

Q525 ***Chairman:*** Mr Schneier, thank you for coming to see us. We very much appreciate the opportunity to talk to you. Perhaps you could first introduce yourself.
Mr Schneier: I am Bruce Schneier. I am basically a security technologist. I write; I speak; I do a lot of thinking in security and how security fits into society. My background is from cryptography, to computer security, to more general security. I had a company in the United States, Counterpane Internet Security, which last October was purchased by BT. So now I am a BT employee. It is important for you to realise two things. One, I am here not as a BT employee but as a security expert; so what I am saying is me and not the company position. Two, I am an American and so my perspective is very much the American laws and the American experience; so I might get some of the UK perspective off. Those are my two caveats.

Q526 ***Chairman:*** Thank you for that. We fully appreciate that although Counterpane, the company you founded, has been acquired by BT and you are now an employee of BT, we are talking to you today in your personal capacity, not in any way as a representative of BT.
Mr Schneier: Excellent.

Q527 ***Chairman:*** Let us get into the questions then and let me ask the first question. Is it possible to put a figure, however approximate, on the cost to the global economy of the insecurity experienced by those using the Internet? What are the main categories of cost and where are they borne?
Mr Schneier: It is a hard question and everyone tries to answer this, because everyone wants to know what are the costs of insecurities. It is hard because a lot of the costs are fuzzy; a lot of them are not well known. We do not have the kind of data you might have on bank robberies or conventional street crime. When you look at the costs, there are the direct financial costs. Right now the big crime is identity theft and there are significant costs. In the US, it is now being said that the amount of profit is greater than the drug trade. That number is being bandied about. It is very hard to know if that is true, because real numbers are hard to get. How much of it is Internet-borne versus "just happens to use the Internet"? Certainly it is in the billions, and direct money is being stolen. When banks are broken into through cyber means they often do not publicise the losses, and so we do not have access to any of that data. A lot of companies keep this secret. There are direct costs also in proprietary information. There is lots of anecdotal evidence that it is not really good to release a lot of data as to how much that costs. The other class is loss of productivity, loss of time. You will see this in the media: "Big Worm Hits", and it is tens of billions of pounds in damage. That is calculated by how many hours did it take for people to get rid of it, times how much they are paid, and that is how much it costs. Of course, these people are paid on salary and they are working overtime; so are those costs real or not? It all depends how you count. A loss of productivity: if your email is down for a day, there is a loss there; but how much do you make up? Amazon knows literally to the penny how much money they lose if their website goes down. They know their throughput. But, much to everyone's surprise, when their website goes down for an hour they tend to make that money back over the next day or so. The customers do not leave and go elsewhere; most of them just say, "Oh, the website's down. I'll try again later". So do you really count those costs? That is hard. There are therefore those indirect costs. There is another class of costs, which I call the "fuzzy costs"—the reputation costs. There are some very public breaches that cost companies their good name. A good example was in the United States a couple of years ago. There was a breach of ChoicePoint, a data broker, and 165,000 personal names and information were stolen. That company took a very serious hit in their stock price, and you could make a very good argument that was directly an effect of the attack. How much is the brand of a bank worth? So there are the costs there. There are also insurance costs that companies are paying. You could look at the entire cost of the security industry. In effect, all the security products you buy are making up for the bad products you have to protect, and that is a multibillion-pound industry. So you look at it that way. It is real hard to

get a handle on the numbers, but that is a flavour of where they might be.

Q528 ***Chairman:*** Do you have a feel for the problem that there is to the individual? We are mainly interested in personal Internet security. Personal identity theft is very troubling for people. I assume that must consume a great deal of time. Would you have any idea about the number of people who never get it resolved?
Mr Schneier: No, we do not know. There are identity theft numbers that are out there. One of the problems is that the definition of identity theft has been changing, so it is hard to get a handle on. The US Government publishes numbers. I do not know what they are, but I know they are published. What exactly do they mean by identity theft? If I steal your credit card out of your wallet and go use it, that is identity theft but it is not what we are talking about here. We are talking about someone impersonating you to a bank, getting credit, getting loans. We have had examples of somebody going away on vacation; they come home and their house has been sold, because someone impersonated them in the real estate market and sold their house. They are very hard things to unravel. Numbers are tough. I think that the US really has a very bad way of dealing with credit reports, credit ratings, and how regulated the industry is. It can take years for someone to restore their good name. In many cases, the money lost is eaten by the banks and the credit card companies, and that is relatively straightforward. It is the time to restore your good name and the stress. It takes people years; they cannot get loans; in some cases their car gets repossessed, even though it is not them; there are arrest warrants out for them. That is what takes a huge amount of time. Putting a dollar figure on that is very difficult, but that is the real cost to the individual. When people are scared, that is what they are scared about. In the US, if you lost your credit card it is a $50 maximum charge to you as an individual; but if your credit rating gets trashed, the effects are enormous; they permeate all through your life. You have trouble getting a job; you cannot get a loan; when you try to rent an apartment, you are not able to. It really affects you.

Q529 ***Lord Young of Graffham:*** What do you understand by "personal Internet security" and who should take responsibility for it?
Mr Schneier: I think that there is a lot of responsibility to go around. The way I often look at it is who can take responsibility? It is all well and good to say, "You, the user, have to take responsibility". I think the people who say that have never really met the average user. I always use my mother as an example. She is not stupid; she is very intelligent, but this is not her area of expertise. If I tell her, "You have to be responsible for your Internet security", she will not be able to. It is too technical, in ways she cannot deal with. So I think that there is a role for the individual, but I like the notion of credit cards. You, as an individual, are responsible for the first $50 and the rest we force the credit card companies to take. This is interesting. Even if you as an individual take your card and fling it out of the window or hand it to somebody and say, "Here, use it", you are only liable for $50, even though you did all the things wrong. The reason that was done—I think it is actually very brilliant—is because the credit card companies are able to solve the problem. Once that law is passed, the credit card companies invest in technology. You can go through that. We used to have books of bad numbers; now there is online real-time verification of fraudulent cards. Cards are delivered in the mail separately from the pin that activates it. You have to call and manually activate a card. There are expert systems that look through the database of transactions, looking for fraudulent patterns. I travel the world. I have used my card in four countries in one day. I was in Winnipeg, Canada, last year and my card was stolen. I used it in a restaurant and somebody copied the number and made a forged card. In two transactions, Visa cancelled my card—and I am amazed. So I think there are some things that we make the user do. Then we have to look towards who else can do it. I think that the ISPs for home users very much should be responsible. Not that it is their fault, but that they are in an excellent position to mitigate some of the risk. There is no reason why they should not offer my mother anti-spam, anti-virus, clean-pipe, automatic update. All the things I get from my helpdesk and my IT department by virtue of being a BT employee they should offer to my mother. I do not think they will unless the US Government says, "You have to". I think that there is a place where the responsibility should be there. Going back, I think that the financial institutions need to bear a lot of responsibility. Here is the problem in the US. Someone gets my personal information, goes to a credit card company with my details—and in the US credit cards are very easy to obtain, so it is a much more pernicious problem than in the EU—and get a credit card in my name. So damage has happened to me and I do not even know about it. I was not involved in the transaction at all. The credit card company should be responsible for that and should be forced to make me whole. They should be the ones to go through the stress of restoring my good name, not me. That makes sense. I would like to see some responsibility on the software vendors, the operating system vendors, the hardware vendors. We are paying the price of insecure software. There is—and I make this up—a vulnerability in an application program or operating system. Someone uses that to hack into my mother's

computer; put a Trojan on the computer; it sniffs her password, and now steals money out of her account. You cannot say that the software vendor is 100% liable for this, but I think it is equally true that they are not zero per cent liable. There is a piece that they can do. When you start looking round, there are a lot of places where you could take responsibility. All the companies really want to push it off; they do not want it. But if you give it to them, like the credit card industry, then capitalism takes over. Once they have the responsibility, they are now going to figure out how to solve it cheaper, better, faster, smarter—and we will get good solutions.

Q530 ***Lord Young of Graffham:*** If we are talking about personal Internet security, we are talking about the average "silver surfer" using it at home. It seems to me that there are three areas. First, I am responsible for the hardware I buy. Occasionally there are hardware faults that give leaks in firewalls. Secondly, I am responsible for the software I use. Thirdly, it is how I use it—so if I leave my password insecure. There are those three areas, therefore. How do I distinguish between my responsibility and the responsibility of the hardware vendor and the software vendor? Those are the two main areas.
Mr Schneier: I think it is hard and I think this is where the tort system really works. I am not an attorney but recently—because I am looking at the legal aspects—I read a book on torts. There are incredibly complicated case histories of partial liability and who gets what. It looks like the system, although it is not easy, sorts that stuff out: how much of it is the user's responsibility; how much of it was the hardware, the software, the website, the ISP in the middle, the DNS server here or some other user over there. You can have examples of DNS attacks, where the company was not even responsible; that some other attacker attacked a named server held by a public organisation, redirecting traffic from the bank to this now phoney bank website. I am entering my bank details; I am fooled. It would be hard to say that I am responsible. There are some visual cues that I might or might not be noticing. These are very hard cases, but I think that we need to start poking at it. We need to start peeling it away. It is probably many years, in different litigations, before we sort it out.

Q531 ***Chairman:*** What you are saying basically is that, while the responsibility is distributed, you think a formula can be made up to distribute that almost quantitatively. So if you have a certain problem, then it is either the ISP provider, or it may be you, or it may be your software manufacturer, or it may be your hardware manufacturer.
Mr Schneier: And it could be a combination of things, like you see in some other areas of tort. Automobile liability—is it the fault of the driver, the automobile manufacturer, the part manufacturer, or the road conditions? There are standards of care that are brought to bear; there are safe driving practices that we expect from people; there are safe road conditions. Investigations are made, the parties come into a room and demonstrate, "I did this and therefore I'm not liable" or "I did this" or "You didn't do that". So it is less that there is a formula; more, there will be a recipe for figuring who did what. It is likely to be relatively standardised. I think that a lot of these frauds are very replicable; that they are not one-offs; that when you see an attack that works, it happens again and again. Attackers change tactics depending on the defences, but the primary fraud is the same. Opening a credit card in my name is a very standard thing that is done.

Q532 ***Lord Young of Graffham:*** Could I come on to e-banking? A personal experience—my daughter had an account with one of the big banks broken into, money taken, and the account was closed. The bank obviously paid up in those circumstances, but is e-banking safe? We are becoming more and more reliant on the use of e-banking.
Mr Schneier: "Safe" is a relative term. To me as a user, if I am not liable, then it is safe. The bank, as a business, decides—however many basis points their fraud is. If you look at credit cards or cheques, fraud is not zero but it is a cost of doing business. You are going to have the CISO of PayPal here. Ask him how many basis points fraud is, and I will bet you that it is under one per cent. It is something that they are trying to get down, but they are a profitable business even though that fraud is there. So the question for the user to ask is, "Am I liable?". If the bank said to me, "We are going to give you a password and if money comes out of the account using that password you have to pay it, regardless of whether you did it or not. You are liable for all withdrawals", I will say, "I don't want that password", because I do not know what the bank's security practices are. I cannot control them. The bank can do something. A file gets broken into, a password is stolen, my money is taken and now I am at fault. If the bank says, "Here is a pin and only withdrawals you make will you be charged for, and any you dispute we will give you the benefit of the doubt", then suddenly I am okay with it, because it is not my risk. The real question is who bears the risk. ATM cards are another example. If there are fraudulent ATM withdrawals from my account, I call my bank and they reverse them. They will probably pull the tapes, look at the video recordings, see who actually did it; but I have the benefit of the doubt there. So I am perfectly happy with my bank card. If it was the other way, I would be less happy.

Q533 ***Lord Young of Graffham:*** Do you think things are improving or becoming more difficult?
Mr Schneier: Things are becoming more complicated. I think the jury is out on whether they are getting better or worse. By any metric, the numbers are getting worse. Fraud is increasing; loss is increasing; damage is increasing.

Q534 ***Lord Young of Graffham:*** But volume is increasing too.
Mr Schneier: Yes, volume is increasing too. Definitely the criminals have found the Internet as a very good place to steal. One of the reasons is because it is so easily international. We actually see jurisdiction shopping. Organised crime will find countries with poor computer crime laws, easily bribed police, no extradition treaties, and they will launch their crimes from there. We see a lot—at Counterpane we are monitoring—from sub-Saharan Africa, from Eastern Europe, from South America, from South-East Asia. So I think it is a growth area in crime. We are seeing much more personal identity information being stolen, but a lot of that is because you steal them in bigger batches now. It is not that there is not a lot of evidence that there is more crime there; I think there is. I think that companies are getting a better handle on fraud. Again, you will have PayPal here and they are great people to ask about stuff like that. PayPal is a monster target out there, because their business is transferring money over the Internet. What better target for an Internet criminal? I will bet that their fraud has been going down, because they are getting better at policing what they are doing. Sometimes you will see measures that banks institute that do not reduce fraud but they move fraud around from one bank to another and then, when all banks are up to this level, a new tactic is developed. So things are definitely getting more complicated. I would say that on a personal level they are getting better, because companies are very scared of all users losing faith, saying, "Oh, it's not safe to buy on the Internet". If that happens, it will be a huge loss.

Q535 ***Earl of Erroll:*** Can I quickly ask a question on banking first? One of the problems in the UK with banking is if the bank felt that the person had given away their PIN number, because they had written it down and someone had seen it, they denied all liability and they were refusing to release details whether it was possible at all. The default position was that the banking system must be secure because the banks would not release information on it. Did you have that trouble in the States?
Mr Schneier: In the States, it appeared from the beginning that they followed the credit card model: that the bank had to prove that you had committed fraud. I think that is a much better model, because the user has no ability to prove that he did not give away his PIN.

Q536 ***Earl of Erroll:*** That was the problem here.
Mr Schneier: In the US the bank cards very quickly followed the credit card model, and I think that was very brilliant. In fact, in a lot of ways in the US—and I do not know if it is true here—both models go through the same systems. If I go to a store and I pay with my bank card or my credit card, it is the same swipe machine. It is the exact same system.

Q537 ***Earl of Erroll:*** It is the same here, yes. On a completely separate issue, you have long been an advocate of holding software companies liable for flaws in their products. Why would this be a good thing?
Mr Schneier: This gets back to putting the responsibility for the problem on them to go back and fix the problem. I will give a very broad explanation. We are paying, as individuals, as corporations, for bad security of products. We are paying it in after-market firewalls, anti-virus, buying Counterpane services, and everything else. It is a huge industry. It is costing us a lot to have insecure software. If we put the liability onto the vendors, it would be expensive but they would either invest in better-quality software development or longer development cycles; they might have to buy insurance; they would certainly charge more for their products. So there would be a cost to that also. But in this second way, in this other cost, the software is improving. Right now, we have a situation where the software is poor quality; we buy these after-market products; the software does not get any better. I want to see the liability moving onto the vendors, to give them a bigger impetus to fix their products. Most of the costs are an externality. The software vendor has an insecure product: the cost is borne by us users. There are several ways you can move the liability back. You can do it through regulation; you can do it through liability that forces the software vendors to spend more money on security, produce more reliable products, and we all benefit. In general, that is why I think that is a good idea.

Q538 ***Earl of Erroll:*** Just to clarify, by "vendor" you do not mean a third-party intermediary; you mean the original manufacturer of the software?
Mr Schneier: No, I mean the manufacturer. In US law—and this happened in the 1920s with automobiles—you would buy an automobile from an independent car dealer and you had a problem with it. You could only sue the car dealer; you could not sue the vendor. That is the notion of privity. That was changed in the 1920s with the very famous case of *McPherson vs. Buick*, which set the precedent that you as the individual could sue the auto

manufacturer and not the dealer. The idea was that the auto manufacturer could fix the problem. Similarly, you need the same thing with software. It is the person who designed, wrote, built the software, the hardware.

Q539 ***Earl of Erroll:*** I am not sure we have the same legal system here. I know that for a lot of stuff you sue the person, and to us the vendor is the retailer of the thing, not the original producer or manufacturer. That is a slight sidetrack, because one of the things that has come out from previous witnesses is that it is virtually impossible to produce software without some flaws in it. You then also get a mix of software on an end-user's system which will be interrelating in unpredictable ways. How do you decide where the liability lies? Surely it will just make the whole thing impossibly expensive or impossible for people to produce new software?
Mr Schneier: I do not think that "difficult" is a reason not to try. Certainly those are issues. I think that we are expecting flaw-free software. I can tell you as a security expert that we in the industry have no idea how to design flaw-free software. We cannot do it. We can do a much better job. If you look at the software development processes in aircraft manufacture, avionics, or in the space shuttle, they are completely different from mass-market software. It probably is not appropriate for mass-market software, but there are things we can do. Even that software is never flaw-free. There have been rockets that have blown up. An Ariane 5 rocket is an example that comes to mind. We can do better, however. This is one of my problems. There are lots of secure development tools out there that are not being used; because, when push comes to shove, there is budget, you have to get your product out quickly, and security takes a back seat to features, to getting it out there. So more pressure on the vendors to do a better job—not a perfect job—because there will be some standard of due care; some standard that you follow.

Q540 ***Earl of Erroll:*** Alan Cox pointed out to us that what would probably happen is that then people will lock down their software and prevent third-party software interacting with this. Of course, that means that you do not get so much innovation; you also cease to open up the software and you get these big hegemonies, like Microsoft.
Mr Schneier: My guess is that the companies protest a little bit too much; that in fact innovation is so profitable and so valuable that you will see it. I think that companies do not want to think about liability; so they are going to produce all these "doom" scenarios. My guess is that, when push comes to shove—just like in automobiles—there are after-market products. I think that it will reduce innovation somewhat, but I am not convinced that the new version of whatever software, with the 2,000 new features you will never use, is always a good thing.

Q541 ***Earl of Erroll:*** That is looking at the products from the big companies. What about open-source software? Who will be liable for that?
Mr Schneier: In the United States we have something called a Good Samaritan law. It basically means that if you see someone on the street, dying, and you attempt to save them, they cannot sue you. That is called the Good Samaritan law. I think there is a model there: that if I produce software for free and put it out there, there is some kind of Good Samaritan law going on, and if you use it there is no liability. If I choose to sell it to you, that is different. Then you can imagine companies, like Red Hat or other companies, taking free software, aggregating it, selling it—with support and with liability. I think that free software is not affected if you do this right. Then you also have a market for companies who take free software and verify it, or somehow build an insurance scheme around it—which you sort of have today, with companies like Red Hat dealing with free operating systems like Linux.

Q542 ***Earl of Erroll:*** What about shareware?
Mr Schneier: I think shareware is the same way.

Q543 ***Earl of Erroll:*** Because you have paid something voluntarily for it.
Mr Schneier: Right.

Q544 ***Earl of Erroll:*** At the moment you paid, you would have a contract?
Mr Schneier: No, I think because it is voluntary; it is a contribution. It is much more like a charity.

Q545 ***Earl of Erroll:*** So that would be Good Samaritan law?
Mr Schneier: Yes. The devil is in the details here. You would need someone who is an attorney to work this out, but I think that general philosophy would work here.

Q546 ***Earl of Erroll:*** What worries me about it is this. I used to write software. If you take the first program I wrote, which was a rational formulation for feeding a dairy cow, I wrote it in my spare time in order to learn how to write a program, and it was the first commercial bit of software I wrote, sold by a particular company. That may well have had 1,001 flaws in it—now, when you bolt it onto something like the Internet. In those days we did not have the Internet. It was not written to be Internet-worthy, because it was doing a specific job. You will kill innovation like that, where people have a specific skill in a specific area and are not having to look at the

global security, about pushing stacks and causing buffer overflows.

Mr Schneier: I do not think you will, but I think you will spark an industry in sandboxing—which is a concept we use of taking a program and putting it in a safe area where it cannot affect everything else. So if you are the modern-day you, writing this piece of software and knowing that you cannot guarantee it is secure but you want to sell it anyway, maybe there is an after-market product where you take your software, put it in, wrap it around, and that provides the security. To me, as soon as you set up these economic incentives, capitalism just solves the problems. Innovation is going to work. There will be hundreds of security products, of security add-ins, of security toolkits. The software toolkit you will use to write that product will do the security automatically. All these things will exist. They do not exist today or they are not commercially viable today, because the market is not there for them. As soon as we say to the software vendors, "You take responsibility for your code", then the after-market, instead of trying to sell my mother a firewall, an anti-virus and all those end-user things, will go to software companies and sell *them* a bevy of products. I would rather see that, because the software companies are going to be smart about buying them.

Q547 ***Lord Paul:*** Are security breach notification laws helpful?

Mr Schneier: I do not know if you have one in the UK. In the US they are very spotty. California passed the first one. I think something like 27 states have followed suit. There is a federal law percolating through the works. It has not been passed yet. It has done a lot of good, but you could also argue that it has outlived its usefulness. Here is the basic idea behind security breach notification law. Companies like ChoicePoint have my personal data. I have no business relationship with them. If, when they lose my data, I suffer, I cannot do anything to them. By forcing them to tell me, we are doing a couple of things. We are notifying me, and we are making them look bad in the media. This is not a joke; I am really serious here. They were making them look bad. It is a public shaming. When the California law was passed, the first big disclosure was ChoicePoint. After that, CardSystems—40 million names stolen. These had huge play in the press. The companies looked very bad. They improved their security. By publicly shaming the companies we sent them to do better, to have better security. That worked really well. The problem is this. In some ways, the media are complacent in making this work. After 20, 30, 50, 100 breaches, the media stop writing about them. In the US we may have three or four security breaches a week, which never get any press. Occasionally one does. If it is a government agency it is more likely to get press. If it is tens of millions of names, it is more likely to get press. There is an attenuation effect. They were valuable but they have become less valuable. At the same time, if you speak to someone in California, he is getting all of these notices in the mail that his innovation has been stolen, and nothing is happening. So he now believes that there is not a problem; he stops reading them. The law was very valuable and it did a lot of good things. The first question you asked me was "How bad is the problem?". It gave us hard data on losses, but it really has outlived its usefulness in the United States. I think that it should still be done, because forcing companies to go public with the information is very valuable—to researchers, to policymakers—but as to the primary value, the public shaming, it is no longer news when someone's information is stolen. It happens too often.

Q548 ***Lord Paul:*** The banks argued to us that reporting the loss of private data would increase anxiety and that customers were being bombarded with warnings. They felt that the companies should decide for themselves about the likely level of harm and about whether it was necessary to inform their customers.

Mr Schneier: Of course they will say that. By definition, you do not want them to decide, because they are the ones who will decide, "Oh, we shouldn't spend the money and risk losing our customers". This is exactly the area where self-regulation will not work. Remember, it is in the companies' best interest not to publicise it. Before the law, we never heard anything, ever. We know what it looks like when companies decide for themselves: we never hear anything. Then they pretend there is no problem. It is only through the laws that we now know it is a problem and how pervasive it is. I do agree that, with lots and lots of notices, it is really a boy-who-cried-wolf problem. After the fifteenth notice, you just stop reading them; but I think that there is still value here. One of the things I want to see in the United States is this. We can do something called a "credit freeze" where, if we have our identity stolen and we are at risk, we can write to the credit bureaux and say, "Freeze my debt information"; that, if someone requests it, I am notified; that if someone overcharges on my credit card, I am notified. I think that if Company X has a million credit card numbers and they are all stolen, they should pay for that service for the people whose names are stolen for a year or so. That seems like a perfectly reasonable thing to ask.

Q549 ***Earl of Erroll:*** Is also its primary use in notifying the authorities of the scale of the problem? Maybe it is not necessary to mail every single person who has just had their date of birth removed and their address, because that has gone about 20 times

already; but it is very useful to the authorities to know who may be operating in which companies, stealing data. So it might be useful to have such a law for that purpose.

Mr Schneier: It does have value there. I think that there is enormous value there. What industries are better or worse; what sorts of regulatory environments are better or worse. In the United States we have our little state petrie dishes: we have slightly different environments, and you can learn what works and what does not.

Q550 ***Chairman:*** Are there authorities monitoring loss of data? If a bank accidentally has a loss of a few thousand names, they might say, "Nobody is going to know". Is there somebody looking?

Mr Schneier: Not really. The law will say that in these states you have to report. I do not think that there is a lot of verification of whether they do or not. I believe that most companies are honest about this, simply because the employees know that it is the law and it is the right thing to do; but there is not a lot of verification. There is not a lot of follow-up on what happened to those names. To me, that kind of data would be very useful: to follow a particular loss; how it happened. This is the fundamental problem. If I had been here two years ago and if you had asked me, "How should users protect themselves from identity theft?" one of the things I would have said would have been, "Shred your trash". That information today is obsolete. Nobody steals personal details, one at a time, from the trash any more; they steal them by the thousands, by the millions, out of these databases. So if you as a fraudster want ten or 100, you cannot get ten; you have to get a million. They do not come in smaller blocks. This is one of the problems. Most of the information stolen is never used, because you only need a little of it. There is only so much fraud you can do; your throughput is only so great. But there are economies of scale, and we are getting better.

Q551 ***Lord Mitchell:*** You have touched on some of these issues, but it is particularly to do with regulation. Do you think that it is likely to improve personal Internet security, or should we be able to change incentives and leave the industry to self-regulate?

Mr Schneier: I think that changing incentives is regulation. I do not like to see regulation that says, "You have to have this brand of firewall, these settings, and do this". I do not like regulation that focuses on the how; I like regulation that focuses on the what. To me, the value of regulation is to set the playing field. A regulation might be, "ISPs are responsible for end users' viruses, zombies, botnets"—whatever. I am sort of making this up. That kind of regulation now forces the ISPs to invest in the technology to do it. It is some of each. That is regulation that sets the playing field. Regulation might say, "Software vendors are liable for flaws in their products that cause losses". That is a regulation that sets the playing field. Less so, the regulation that says, "Here is how you fix it". Environmentalism is a good analogy here. I like to see regulation that says, "The maximum level of this pollutant is 'x'. How do you achieve it? You could shut down your factory. You can buy scrubbers. How you deal with it, we don't care"—rather than regulation that says, "You must use this type of scrubber in your smokestack". To me, regulation that sets the playing field is very valuable. Another thing government can do—and we are starting to see it in the United States—is use its buying power. The United States Government buys an enormous number of computers, operating systems and application software. It can start making security demands on these products. The benefit of the software industry is that the first copy is expensive, all the rest of them are free. If the Government says to an operating systems vendor, "You must have this type of security", the operating systems vendor does it—and we all benefit, because now it is embedded in all of its offerings. Right now in the United States there is a procurement going on for an encrypted laptop. One of the problems we have is that government officials lose their laptops and government secrets all the time. I am sure you have the same problem. So the Government, under the auspices of NEST, is holding an open competition for encrypted laptops. Software vendors will be submitting their products. I am not sure how it is going to work. This is phenomenal. This will force all of the vendors to produce a product; to have some very good government standards; the winner will get an enormous PR boost; all the losers will fix their products—they lost, but they will do better next time—and we all, even people in the UK, will benefit because those products will now be for sale. That is a huge way in which government can help. Instead of governments buying firewalls, routers or application programs, they could put in a demand requiring a secure software development—and we all benefit.

Q552 ***Chairman:*** The great advantage is that the cost of the item that holds the software is basically zero. You do not have inventory problems, do you, because the plastic disks are worth nothing? If you want to upgrade your software because you have been forced to upgrade it, that can be done at very little cost, can it not?

Mr Schneier: It is not even plastic disks. These days, I buy software online. The cost is zero. Upgrading can be hard. We live in a world where we have lots of security patches, and we find that the take rate of patches can be low—and that is unfortunate. We are doing better. Patching is a very hard problem. If you

think about the way the patch works, it has to be incredibly quick. You want to get that patch out as quickly as possible. At the same time you have to test it in every possible configuration, and you cannot do both. Those are incompatible requirements. Companies—Microsoft is an example—went to a system where they released their patches once a month. It is called "Patch Tuesday". They batch their patches, test them well, and release them once a month. On the one hand, that increases the length of time that a system is unpatched, and that is bad; on the other hand, the patches are much more reliable; users are much more likely to turn on automatic patching and, overall, we get better security. The cost to push those upgrades down is not zero; it is there, but we are getting better as an industry in doing that reliably, effectively and efficiently. If a regime of liabilities comes in, software vendors will get even better at that, because they will have to. We are doing better than we were, but there is still a cost to upgrading software in the field. There is stuff that you cannot upgrade. Cisco routers—there is no upgrade path for some of that. The way you upgrade is to buy a new one. When there is a vulnerability found in them, you are stuck; there is nothing you can do. That is not true for a lot of software; it is true for some of the appliances.

Q553 ***Lord Mitchell:*** In the attempt to have this level playing field which you talk about, is there some way that regulation can keep pace with technological change? It always strikes me that all the regulators and the legislators are light years behind what is happening in the real world.
Mr Schneier: I think the trick there is you legislate results, not methodology. So, yes, the legislation will never keep pace with technology, but the legislation should say that fraud is illegal, however it is done. Identity theft is illegal. You have to take responsibility for bad things that you cause, whatever the technology. So it is not technology that covers streaming music or particular things, but legislation that is technologically invariant—that is the best. You are right: we are not going to know the criminal tactics, the ways the Internet will be used, where the threats come from, the particular technological configurations, but crime never changes. We talk about identity theft like it is a new crime, but it is not. It is fraud due to impersonation. There is English common law on these problems. What is new is the regime where it is playing out; the economies of scale; some things are easier, some things are harder; but the crimes are essentially the same. One of the problems we have is denial-of-service extortion. This is a new area of organised crime. We are seeing more of it in companies we monitor. Organised crime will have a bunch of zombie computers. These are computers, controlled that they can use to send track out. They will extort money. They will attack you, drop your servers, and then demand you pay up or they will do it again. This is extortion. It is not a new crime; it is an old crime. I want the laws to be written so that they are invariant to technology. If we do that, I think we will be okay. We have a problem in the US with eavesdropping. All of our laws are written about telephone eavesdropping. They are all "telephone, telephone, telephone". Now people chat on email, on SMS, on voice-over IP. Guess what? The laws did not apply. If the laws are written to apply to conversation by whatever means, then it does not matter what you invent in the future: the laws apply. The laws have to be written well and, if they are written well, I do not think there is a problem.

Q554 ***Lord Young of Graffham:*** Our machines get upgraded. It seems to me that every time I switch it on, twice a week, it has been upgraded overnight. But if I do not change my password or, worse, do not put a password in the day I get it—I just cannot be bothered—whose responsibility is it then? It is my responsibility, is it not?
Mr Schneier: I do not think so. If your computer is sitting in your house and the door is locked, the key in your front door is your password. Do you mean a special computer password?

Q555 ***Lord Young of Graffham:*** Yes.
Mr Schneier: I have a computer at home that has no password, because I consider it is in the secure perimeter of my home. It is different from a laptop computer, which is right now in my hotel room. There is a very different set of security assumptions going on there. Even if there is a password, that does not mean you are safe. Lots of things can be done anyway. Passwords are much easier to break these days. I did an essay on this about a month ago. There are companies that sell software that break passwords. They sell to law enforcement; they sell to companies. Employees that leave or get fired or, in worse cases, die—they need to recover their passwords. So there is methodology for password recovery. Passwords do not mean "safe". They are a barrier to entry: in some cases not a very good one. So be careful. Do not look at the technology as that you did this magic spell and therefore you are safe. Everything is a barrier, and they all seem to be surmountable with enough effort.

Q556 ***Lord Young of Graffham:*** Thank you. You have saved me a certain amount of effort in the future!
Mr Schneier: You know the joke about not having to outrun the bear, but just having to outrun the people you are with? In a lot of ways, security for the home is like that. If I am more secure than the people next door, the criminals will go there. If my company is

more secure than that company over there, the criminals will go over there. As an individual or as a company, my goal is not to reduce crime; my goal is to move it over there, without that happening to me. From your perspective, that is not good enough. You want to reduce crime, because if you just move it from one town to the next that will make no difference. It really depends on the perspective.

Q557 ***Lord O'Neill of Clackmannan:*** Do you think the Internet is well policed?
Mr Schneier: The Internet is better policed than it ever was. The Internet is by nature hard to police. The international nature makes it extremely difficult. Most of our crime laws are based on proximity. I walk up to you, hit you over the head with a rock and take your wallet. That is how we envision crime. That is how our laws work. Internet crime very often breaks international boundaries, goes into countries that have not very effective police, and it makes it hard to police. It can be very hard to prosecute these cases; they are very technical. It can be hard to prove someone was guilty. You can prove that the attack came from my computer, but how do you prove that I was the human being in front of the keyboard, directing the attack? Maybe my computer was owned by a computer in another country and the attack just came through my computer. It is very hard to prove. All that being said, we are much better than we were years ago. The law enforcement agencies in the United States, in Europe and in Asia have gotten much more savvy about Internet crime and how to deal with it. Our investigation tools are better; there is a lot more international sharing of information. So we are getting much better at it. This is the other half. We spend the entire time talking about one side of computer security: what can we do to prevent the bad things? The other side—how do we make the people who do the bad things not want to do it any more?—I think is equally important. Policing the Internet, putting criminals in jail, will go a long way to making the Internet safer. Just as we say we can never make the Internet perfectly safe or software perfectly secure, we are not safe against murder when walking through the streets of London; but because we live in a lawful society, because there are police, because people know if they commit murder they are likely to be caught and put in jail, that reduces the crime rate such that I am not wearing a bullet-proof vest and I feel safe not wearing it. I think there is a huge amount more that law enforcement can do, nationally and internationally, but we have made enormous strides. In some ways I am really proud—I know much more about the FBI than any place else—of the work they have been doing in making themselves smarter on computer crime.

Q558 ***Lord O'Neill of Clackmannan:*** Would it be right to say that at one time it was almost beyond the law but it is now within the law?
Mr Schneier: There are times when you could say that it was kind of like the Wild West, which is the American metaphor of local purchase law. That if you, as a community, as a business, could hire your own law, you could be safe; but out in the world it was just a complete mess. It is not that bad any more. I think that it is much better than that. There are still aspects of that, but it is better. Actually, the PayPal people will also talk about this. There is a dollar threshold in the United States before the FBI will get involved. Criminals know this, and so they are more likely to do small amounts of fraud to a lot of people than large amounts of fraud to a few people, because they can stay below the FBI's radar. Clearly something has to be done about aggregates, therefore. There are a lot of ways in which law enforcement can do better, but I think that we have done an enormous amount. If you look back ten years ago, the FBI was completely clueless.

Q559 ***Lord O'Neill of Clackmannan:*** I am not asking you to pass comment on the law of the UK, but is there any way of ensuring that the law can be obeyed online?
Mr Schneier: Can be . . . ?

Q560 ***Lord O'Neill of Clackmannan:*** Obeyed, recognised. Are there sanctions?
Mr Schneier: To me, the law is obeyed, first because most people are honest and, second, because there are penalties for not doing so. You need both. There is education on what is the law and how to obey it, and then there are the penalties if you do not. You do not ensure that it is obeyed; you just make sure that, if someone disobeys it, something happens.

Q561 ***Lord O'Neill of Clackmannan:*** Perhaps I could ask you a question about security researchers—yourself. Have you been in a position where, by highlighting the difficulties which some companies have created for themselves, you are flagging up that they are not as free? Does it happen that researchers in the kind of field that you are in, when they do this, are exposed to criminal charges or civil charges?
Mr Schneier: It has not happened to me, but it happens all the time. There is an enormous amount of corporate pressure put on researchers to keep these things quiet. To me, there is enormous value in making them public. Otherwise, people cannot make intelligent buying decisions; the problems never get fixed; the companies pretend they are not real. So there is a huge amount of debate and pressure to keep these secret. In the United States we have had researchers that have been sued; criminal charges have been put against them; they have been

persecuted. I think that this is a huge problem. We need to recognise the enormous value of talking about flaws, of highlighting them. Before we as an industry started regularly exposing these flaws, companies would never fix them. Now even if we do not, there is still the threat. Something in the non-computer area, something that I was personally involved in—in the United States, and it is probably the same in the UK, you can print your boarding passes at home for air flights. Someone wrote a program on the web that allows you to print a fake boarding pass to get through airport security. The FBI raided his home and took away his computers. This was a flaw that I mentioned in 2003; a United States congressman mentioned it on the floor of Congress a couple of years later. These things were public. This person demonstrated it on the web, and he got hit real hard by government. What does that say about us as a community and how we respond to hearing about these things? I think that it reflects very badly.

Q562 ***Chairman:*** He never attempted to make any money out of it?
Mr Schneier: No, of course not.

Q563 ***Chairman:*** Or to do it himself?
Mr Schneier: And I did not either, and neither did Congressman Schumer. We all said, "Look, here's a problem. This exposes how silly this security measure is".

Q564 ***Lord O'Neill of Clackmannan:*** There is a paradox here, is there not? For example, banks are not required to disclose how much they lose, but if someone were to identify a loophole in their system by which such losses are made, they would be hammered but the banks would still remain—
Mr Schneier: Right, and I think that is backwards. If I am a consumer and I want to make an intelligent buying decision on which bank I should use, which software I should buy, I should have as much information as possible.

Q565 ***Lord O'Neill of Clackmannan:*** Short of discouraging people from looking for flaws in the system, do you think there is any way that we could adequately protect researchers, or is it just one of the risks? They are in the jungle, there are big animals there, and they are going to get caught?
Mr Schneier: No, I think researchers should be solicitously protected under laws protecting free speech or academic research. I would like to see protections for researchers. There really is not something like that in the United States. You would do well for the researchers in your country by ensuring that anything they do they will not be penalised for. There are analogues and whistleblower laws that you can look at, but I think that it is really important to have viable research. You learn about security by breaking things. That is the way you learn. If you cannot break things, you cannot learn. The criminals are always going to learn, always going to break stuff. We need to be smarter than them. We are not going to be smarter than them unless we can break things too. I think it is very important.
Chairman: Mr Schneier, we have asked you a lot of questions and you have answered them in a most interesting way. It has been extremely useful to us and we are very grateful indeed to you. Thank you for coming to talk to us.

WEDNESDAY 21 FEBRUARY 2007

Present	Broers, L (Chairman)	O'Neill of Clackmannan, L
	Erroll, E	Patel, L
	Harris of Haringey, L	Paul, L
	Howie of Troon, L	Young of Graffham, L
	Mitchell, L	

Memorandum by eBay UK Ltd

Introduction

1. eBay welcomes this opportunity to comment on the House of Lords Science and Technology Committee's Inquiry into Personal Internet Security. eBay.co.uk was launched in the UK in October 1999 and is now the UK's largest online marketplace with over 15 million registered users.

2. PayPal Inc. was acquired by eBay in October 2002. PayPal (Europe) Ltd is a private limited company incorporated in the UK, and authorised by the Financial Services Authority as an electronic money institution.

3. The eBay group of companies operate 33 websites around the world. In total these websites have over 212 million registered users, with over 15 million in the UK alone. At any one time there are approximately 105 million items listed for sale on these websites globally, and over 10 million of these are listed by UK registrants on the UK website.

4. eBay is a key enabler and driver of UK e-commerce, providing a means for tens of thousands of UK small businesses to get online and trade within the UK and globally. A survey conducted for eBay in February 2006 by AC Nielsen International Research for eBay found that over 68,000 people in the UK and over 170,000 people in the EU depend on eBay for at least one quarter of their income. eBay users range from private individuals, through sole traders all the way up to some of the largest companies in the world, such as IBM, HP and Vodafone.

5. eBay is often referred to as an online auction house, but this term can be misleading and is actually inaccurate. In fact, eBay is neither an auction house, nor an online retailer in the traditional sense.

6. For example, eBay is not:

- involved in the actual transaction between buyers and sellers;
- in control of the quality, safety or legality of the items advertised;
- in control of the truth or accuracy of the listings or the ability of sellers to sell items or the ability of buyers to buy items;
- at any time in possession of the goods listed;
- able to inspect the goods listed.

7. eBay instead provides an online marketplace where practically anyone can buy or sell practically anything. And as a marketplace of buyers and sellers, eBay has an interest in ensuring both strong consumer protection and light touch, proportionate regulation for our sellers.

eBay and Consumer Empowerment

8. eBay empowers consumers by:

- increasing choice in terms of the wide selection of goods available in over 50,000 categories;
- providing a safe environment in which buyers and sellers can trade as well as advice on how to trade safely;
- providing detailed information about the reputation of the seller through its unique Feedback Forum (see below);
- making the comparison of price and services easier for the consumer through greater price transparency;

— making inefficient markets more efficient, in many cases reducing prices; and

— by empowering SMEs to access global markets and compete with larger, more established companies and traditional "bricks and mortar" businesses.

The Feedback Forum

9. Feedback remains a key driver of both trust and safety on eBay by establishing a virtual reputation that can help protect buyers and sellers alike. Based on each unique trading experience, buyers and sellers leave feedback on other members. Members are then able to view in a member's profile their overall rating and positive, negative and neutral feedback left by both buyers and sellers. As of September 2005, eBay members worldwide had left more than five billion feedback comments for one another regarding their eBay transactions. If buyers have a question about a particular item, they can also email the seller and all other buyers will be able to see their answer.

10. A recent Ofcom survey on Online Protection cited eBay's Feedback System as "an example of an innovation to address potential consumer fears about inadequate protection" and as "an example of successful consumer action in tackling rogue traders on the internet".

Trust and Safety

11. The vast majority of eBay users enjoy a perfectly safe trading experience. eBay uses leading edge technology and employs more than 2,000 employees—with backgrounds in law enforcement, customer support, advanced computer engineering and analysis—to help ensure a safe online trading environment for our users.

12. eBay.co.uk's commitment to "Trust and Safety" can be divided into three main areas: education; prevention and detection; and protection and resolution.

13. eBay is committed to educating our users on how they can trade safely on eBay and elsewhere. Tips on safe trading can be found on eBay's Safety Centre, where users can also contact our 24/7 Customer Support representatives and receive advice on any problems they may encounter. Our Safety Centre can be accessed from every single page on the website—as can our Help pages. More interactive tips, advice and tutorials are available on "eBay Explained".

14. In addition to being a member of the Government's Internet Crime Forum, eBay is also a major sponsor of "Get Safe Online"—the UK's first national internet security awareness campaign for the general public and small business. Get Safe Online is a joint initiative between the Government, the Serious Organised Crime Agency (SOCA) and private sector sponsors from the worlds of technology, retail and finance—including BT, Dell, eBay, HSBC, Microsoft, and SecureTrading. Get Safe Online (GSOL) provides free, simple, clear advice to encourage the general public to protect themselves and their electronic devices when online.

15. A recent GSOL survey found that:

— 21% of people rated internet crime the type of crime they most feared, compared to 17% last year;

— 24%, 21% and 18% of respondents have been deterred from internet banking, online financial management activities like arranging a loan and shopping on the web respectively, while 17% say safety concerns have stopped them logging on altogether;

— 72% of people said they would like further information about internet safety, compared to 78% last year;

— when looking for internet safety advice, 35% would go to friends or family, a quarter would go to an internet safety website such as www.getsafeonline.org and a fifth would turn to their ISP;

— 40% are still not sure where to go for this advice, an improvement from 48% last year;

— 51% of people use the same password for more than one website and 17% use personal information about themselves in passwords, leaving themselves more at risk from hackers;

— 83% of people now have anti-virus protection on their PCs, but a fifth haven't updated it in the last three months;

— Less than one quarter (24%) of people think it's their own responsibility to safeguard themselves online. Forty one per cent think the big online companies should insure their customers against fraud;

— 52% of internet users questioned do their banking online, nearly a third (32%) pay their utility bills online and almost a quarter (23%) buy their groceries online.

16. An industry wide safety concern which affects not just eBay but the financial sector relates to identity theft or account takeovers where fraudsters attempt to gain access to eBay and PayPal members' accounts. Our systems detect and remove most account takeover listings before any harm is done, and we now offer a Live Chat facility to provide urgent assistance for users who suspect that their account has been taken over.

17. eBay regularly runs "Spoof Protection" campaigns on how to avoid spoof emails and offers online tutorials to help users identify spoof.

18. We have also developed a groundbreaking new Toolbar—which users can download for free from the eBay site—with an Account Guard which warns eBay members when they are on a potentially fraudulent (spoof) website. This feature also enables members to report a spoof website. Once a site has been verified by eBay to be fraudulent, that information is then automatically distributed to all other eBay Toolbar users, warning them about the spoof website.

19. eBay also led the way in adopting the Sender Policy Framework (SPF) industry standard which helps spam filters detect forged email more reliably. This not only increased members' actual level of protection, but also helped the standard achieve rapid penetration in the industry. SPF is now adopted by most prominent Internet sites and anti spam products.

20. Finally, we have introduced "My Messages"—a means for eBay users to send and receive eBay-related communications inside "My eBay", similar to a web-based email inbox. In contrast to regular email systems where many users find it difficult to recognise forged email, users can be assured that any information found in My Messages is legitimate.

Safe Payments—PayPal

21. Safe online payment mechanisms are essential for consumers in an online environment. Offering online users the ability to send and receive payments securely, easily, and cost-effectively is essential to the development of e-commerce. eBay members can pay for items using a variety of different options such as PayPal, credit cards, debit card, personal or bank cheques, postal orders, and other methods. However, it is now eBay policy that sellers may not ask buyers to send cash through instant money transfer services (non-bank, point-to-point cash transfers) such as Western Union or Moneygram. This is because of concerns about the safety of this type of payment mechanism.

22. PayPal can be considered a secure online payment system for a number of reasons:

— PayPal never shares buyers' bank account, debit card or credit card information with sellers;

— PayPal maintains the world's leading fraud prevention system and the industry's most advanced detection techniques to minimise losses, protect members' accounts and preserve customer satisfaction. As a result, PayPal maintains a very low loss rate due to fraud—0.33%;

— PayPal offers Buyer Protection of up to £500 for qualified purchases plus Seller Protection which gives protection from chargebacks due to fraud on qualified transactions (see below);

— PayPal is safer than money orders, because money order companies do not offer fraud protection services or recourse when fraud occurs;

— PayPal allows buyers and sellers to send and receive money quickly and allows merchants to receive payments almost immediately;

— it is always free to send money via PayPal—and for sellers, PayPal has lower transaction fees than most credit card merchant accounts;

— PayPal is also cost effective in cross-border and multiple currency transactions, enabling buyers in 103 markets to easily pay for items and services and allowing customers to send, receive and hold funds in a total of 17 currencies worldwide;

— regulated by the FSA as an e-money institution, PayPal complies with UK and EU regulations governing its business and relation with its customers;

— PayPal users can avail themselves of the Financial Ombudsman Service.

23. PayPal is available as a payment option on eBay as well as on other e-commerce sites.

Buyer Protection and Resolution

24. Where things do go wrong, credit card companies typically provide identity and purchase protection, whether buyers are paying with your credit card through PayPal or directly to the seller.

25. Users may also benefit from eBay or PayPal's Buyer Protection Programmes. eBay Standard Protection covers items that are not delivered or that are "significantly not as described" for up to £120 (minus a £15 administration fee). PayPal Buyer Protection also covers non-delivery of tangible items that are received "significantly not as described" for up to £500, and sellers can enjoy PayPal Seller Protection to protect themselves against chargebacks.

26. Where there are disputes between buyers and sellers, eBay also provides an online dispute resolution facility through third party mediators like Square Trade.

27. Finally, both eBay and PayPal have a specific fraud investigations team who work extensively with official online fraud experts such as SOCA e-crime, and liaise closely with the Police to fight internet fraud. eBay.co.uk also has a dedicated police liaison officer with over 30 years experience at Scotland Yard who works closely with the police in their efforts to apprehend any perpetrators.

Prohibited Items

28. eBay only permits legal items to be sold on the site. Items that infringe legal regulations or eBay rules and policies may not be offered for sale on eBay.

29. In many areas, eBay guidelines exceed UK or international legal regulations. For example, it is permissible to buy airguns in the UK subject to certain legal restrictions, but eBay prohibits any kind of trade in these weapons. Similarly, the trade in live animals is basically permitted by law—but, with very limited exceptions, eBay prohibits any kind of trade in live animals on the market place.

30. eBay complies with all laws related to notice and takedown and we provide intellectual property rights owners, users, law enforcement and other interested third parties with the means to report items of concern to eBay. But with over six million new items listed for sale every day, it is not possible for eBay to monitor and check every item on our site either because of the volume or the expertise required for each and every item. In fact, under the E-Commerce Regulations 2002, companies like eBay who are "information society service providers" generally do not have a legal obligation to independently screen the content hosted on their sites for legality.

31. However, as a responsible corporate citizen, we invest heavily in reviewing reports from third parties and in proactively searching through items—to the extent that we can do so. Because we are not an expert on the many hundreds of thousands of different items offered for sale, we cannot search based upon item specifics.

32. When searching through items, eBay uses leading-edge technology to assist in finding references to certain prohibited items such as firearms, drugs, pornographic material or blatantly counterfeit material (such as items which state that they are counterfeit or replica). As soon as these are identified they are promptly removed from the site.

33. Items that are prohibited may appear on the site on occasion because no searching technology can be 100% effective when run against six million new items a day. It is not feasible to manually review every item and no technological searching process can work instantaneously when these millions of new items that appear on eBay the instant they are listed by sellers—24 hours a day, seven days a week.

34. It has not proved possible to pre-search through items or to automatically end items (without manual review) because of the overwhelming and debilitating cost and the large number of wrongly ended items ("false-positives") which will result. Reporting parties should not expect items to be removed from eBay immediately after they are reported.

35. eBay follows industry best practices when investing in search technology and developing actual filter rules. However, searching technologies are not perfect—they need to be reviewed and modified regularly. It is much easier to identify an individual problem item than it is to convert the item specifics to a rule that excludes false positives. eBay will continue to invest heavily in improvements in this area.

Attacking Counterfeits

36. eBay is strongly committed to help protecting the intellectual property rights of rights owners and to providing our users with a safe and enjoyable place to trade. For this reason, eBay has created the Verified Rights Owner (VeRO) Programme so rights owners can report listings that infringe their rights. Any person or company who holds intellectual property rights (such as a copyright, trademark or patent) which may be infringed by listings or items sold on eBay is encouraged to participate in the VeRO Programme. Currently, the VeRO programme has over 17,000 participants and every week eBay removes thousands of listings at their request. eBay is also a member of the UK Anti-Counterfeiting Group.

Specific Trust and Safety Campaigns

Mobile Phones

37. eBay recently partnered with the National Mobile Phone Crime Unit (NMPCU) to ban listings for "blocked" or "barred" mobile phone handsets on the site, clamping down on the sale of stolen phones. The partnership follows a successful joint-operation in Greater London to identify and arrest eBay users trying to sell blocked or barred phones. The joint investigation by NMPCU and eBay's Fraud Investigations Team led to the execution of 20 warrants and 13 arrests in the Greater London area. Forty-five stolen mobile handsets were seized as part of NMPCU raids carried out on the basis of information supplied by eBay.

38. eBay has now introduced a ban on the sale of blocked/barred mobile handsets on the site. Any reported listings for blocked/barred mobile phones will be taken down as they are in breach of eBay's policy on encouraging illegal activity. eBay also works closely with the National Mobile Phone Crime Unit to eliminate the sales of stolen mobile phones within its marketplace. eBay has also launched an on-site campaign to communicate its policy against the sale of blocked or barred mobile phones to its users. The activity also includes a guide written jointly by NMPCU and eBay to warn buyers of the dangers of buying stolen handsets, as well as advice about how to ensure that a handset is not stolen. eBay also provides links to the NMPCU website and sites like immobilise.comhttp://www.immobilise.com/ and checkMEND.

Antiquities

39. eBay has also recently signed a Memorandum of Understanding with the Metropolitcan Police, the British Museum and the Museum Libraries and Archives to ensure that antiquities found in the UK are being sold legally on its site.

40. In order to prevent illegal sales of treasure, the Portable Antiquities Scheme (PAS, which is managed by the British Museum on behalf of the MLA) has set up a team to monitor antiquities sold on eBay and to ensure that sellers have the right to trade them. Where the listing is illegal, PAS will report it to the Art and Antiques Unit of the Metropolitan Police and eBay, which has committed to end illegal listings. eBay is the first website to reach an agreement with the British Museum and the MLA banning the illegal sale of treasure over its trading platform.

Protecting Members' Privacy

41. A key security issue for consumers when shopping online is privacy. Since 2004, eBay has consistently been ranked as one of the ten Most Trusted Companies for Privacy, according to TRUSTe:

- eBay has always been an industry leader in providing appropriate privacy disclosures to members and obtaining appropriate consent, including, among other things, requiring them to read the privacy policy before they can register to use the website;
- eBay does not share, rent or sell personally identifiable information to third parties for their marketing purposes without a member's explicit consent;
- eBay continuously reviews its privacy practices and modifies its privacy policy regularly to keep up with best business practices and new legislation globally in close co-ordination with its members and privacy authorities;
- eBay also uses encryption, anti-fraud tools, secure socket layers (SSL), and firewall technology to protect consumer accounts and personal information.

— Finally, eBay promotes its privacy practices throughout the website via easy-to-read summaries, charts, principles and its privacy policy. eBay also clearly indicates to members that all questions and discrepancies should be resolved by referring to the privacy policy located at the bottom of every webpage or by contacting our Customer Support department.

UK Regulatory Framework

42. eBay fully complies with all relevant legislation affecting e-commerce. In addition, we provide detailed advice on relevant legislation affecting our buyers and sellers.

43. For example, we provide advice to business sellers of their legal obligations to consumers—for example, in relation to the Sale of Goods Act, Distance Selling Regulations and the Trades Description Act—and link to other sources of advice on consumer rights offered by the Government and Trading Standards Departments. We also provide advice to traders to help them understand the implications of trading internationally and the need to comply with laws in the country to which they are shipping goods, in particular the various import and export restrictions which are in place.

44. However, it is often difficult for small sellers to deal with the compliance costs created by a patchwork of legal rules in different EU jurisdictions. For example, the Distance Selling Directive follows the minimum harmonisation approach, giving all Member States the option of maintaining or introducing a higher level of consumer protection. This approach means for example that "cooling-off" period in which the consumer can withdraw from the contract is seven working days in the UK but 14 Days in Denmark, Finland, Germany, Portugal and Sweden. Similarly, consumers bear the direct costs of the return of non-defective cancelled goods in most Member States, but not in Germany and Finland where sellers are liable for such costs.

"Online Auctions" and the Distance Selling Directive

45. Contracts concluded at an auction are excluded from the Distance Selling Directive (97/7/EC). Although online auctions on eBay have an auction style, they differ from traditional auctions in a number of key respects. Unlike traditional auctions, eBay does not conduct the bidding process using a human agent, nor does it make an assessment of the value or condition of the goods or take possession of any goods to be sold by eBay sellers to buyers. Furthermore, eBay is merely a trading platform for both sellers and consumers, and it is not involved in the conclusion of the contract between the seller and the buyer. Accordingly, eBay is not an "online auctioneer" contrary to what is often assumed. This view has been confirmed by the Germany Federal Supreme Court (BGH).

46. In many Member States however, it is not clear whether online auctions are subject to the exception of auctions in the Distance Selling Directive. This creates legal uncertainty which needs to be resolved.

Conclusion

47. eBay welcomes the House of Lords Science and Technology Committee's Inquiry into Personal Internet Security. We are committed to ensuring a safe trading environment for all our users and to supporting initiatives designed to promote online security.

17 October 2006

Memorandum by the Confederation of British Industry (CBI)

1. The Internet has changed the way we communicate, work and live. Terms such as "blog", "download" and "Google" have become a normal part of our everyday language at work as much as at home. However, unfortunately so too have the terms phishing, spam, spyware, computer virus and identity theft. Internet users are increasingly at risk from a constantly evolving online threat environment. The ever-increasing sophistication and ability of organised criminals, terrorist groups and individual hackers to use the Internet as a tool for criminal activity has meant an increasing importance being placed on the need to protect personal information and business data when online.

2. The CBI welcomes the opportunity to provide input to this important inquiry into personal Internet security. It is important to recognise that the networked economy has grown extensively over the last decade, and with it the interdependence of the online community in the UK. However, all those using the Internet, whether it is for business or personal use, leave themselves and other online users open to online attack if they

are operating insecure Internet systems. Public concerns over Internet security and lack of confidence in using online services represents a key risk to the UK maintaining and building on the economic growth gained from the e-business and e-commerce. Furthermore, the success of the planned transformation of public services' delivery relies on the trust and buy-in of the UK public to the use of the Internet to engage with government.

3. The Internet is a vast network of computers connected together through a series of servers located across the globe. This means that, when considering the issue of Internet security, the Committee cannot confine itself solely to considering the threats and security dangers for private individuals without also recognising how the behaviour of individuals can impact on the Internet security of companies and government agencies.

What is the nature of the security threat?

4. Online interaction between individuals and business has increased in recent years, becoming more extensive and elaborate with firms using the Internet to deliver added-value and innovative goods and services. However, just as Internet users are becoming more sophisticated, so too are criminals. As users and developers of Internet security tools become more aware and savvy of online dangers, criminals are modifying attacks to make them more targeted.

5. The changing nature of security threats can be illustrated by the evolution of spam and phishing attacks. In the past, spam emails were often simply an annoyance to users and computer system administrators. However, spam now poses a serious security risk as one of the most effective ways of spreading malicious software (malware) and computer viruses. Just opening an infected email, which a user may honestly believe is from a trusted source, can may lead a significant damage. Some spam emails are sophisticated enough to be able to block anti-virus systems and actively change to avoid detection by anti-spam technologies. Targeted phishing attacks, involving highly detailed personal information obtained through identity theft to customise emails to make them seem more plausibly sent from bona-fide organisations or individuals, are known as "spear" phishing.

6. As personal information becomes a valuable asset to criminals, identity theft has become a major threat to online users. The increasing online provision of goods and services has led to consumers and firms creating numerous online identities in accordance with the requirements of different online providers. For example, individuals may have a different username and password for online banking than they do for downloading music or booking a holiday online. This situation increases the risk of identity theft, as individuals are required to provide duplicate identifying and authenticating data to multiple companies that are then open to possible exposure and theft. Federated identity management is emerging as a possible solution to this problem as it allows individuals either a single sign-on or a system of multiple sign-ons based on a single set of shared identity data. However, any federated scheme must have appropriate security in place to protect the identifying data that is accessed and shared between multiple partners.

7. The increasing online provision of goods and services has been greatly supported by the popularity of broadband in the UK. According to the Office of Communications (Ofcom) there are now 11.1 million broadband Internet users in the UK, compared with 6.2 million in 2004.[1] The take-up of broadband is welcomed by business. However, the CBI remains concerned that broadband users may not be fully aware of the increased risk of attack when moving from narrowband to always-on Internet access—illustrated by the rise in "botnet" attacks in the UK over the last few years—and the additional security subsequently required.

8. Sent largely via spam emails, "botnets" consist of programmes installed by hackers that enable them to gain control of an online computer; turning the computer into a "robot" or "bot". These "bots" are then used as part of a wide network of computers to distribute viruses and/or launch phishing or denial of service attacks. Botnets thrive on computers that spend large amounts of time online, as they form a more stable network of computers for distributing viruses, spam and phishing attacks. In the UK the rise in broadband "always on" Internet access is resulting in broadband users spending on average 12.7 hours a week online, compared with only 6.6 hours by traditional narrowband users.[2] This means that broadband users that do not have adequate security in place are at increased risk from a botnet attack. According to research published by Symantec in March 2005, the UK already has the largest population of botnets in the world, ahead of both the US and China.[3] With broadband the backbone of the UK's networked economy, raising awareness of broadband security issues must be seen as a key priority for government and business alike.

[1] Ofcom Communication Market Report 2006
[2] Ofcom Communication Market Report 2006
[3] Symantec Global Internet Threat Report March 2005

What is the scale of the problem?

9. It is difficult to assess the true scale or impact of Internet security attacks on the UK as victims, are both often unaware of security attacks and how to report them. Reluctance also sometimes exists amongst businesses to report e-crimes because of concerns over adverse publicity and damage to corporate reputation—another factor is also a lack of confidence in the capabilities of local police forces in responding to and investigating incidents of e-crime. This may be to a certain extent simply a matter of perception. For example, firms sometimes fear that reporting e-crime to their local police will result in the removal of their IT hardware for investigation, leading to an inability to adequately continue conducting business. But it can also reflect a relative lack of skilled personnel and resources within local forces in dealing with online crime. The recent dissolving of the National High-Tech Crime Unit was seen by many businesses as a reduction in the Government's commitment to fighting computer crime. Together, these factors perpetuate a reluctance amongst businesses—particularly outside London—to report e-crime, something that is helping criminals to elude prosecution.

Do the public understand the threat they face?

10. For many people caught up in the straightforward demands of day-to-day life and the tasks of running a viable business, Internet security can seem faraway, just too daunting or purely a technical issue. This is, until disaster strikes.

11. Media coverage of incidents of computer crime and identity theft has raised the profile of online security in the business community. According to the DTI 2006 Information Security Breaches Survey, nine out of 10 UK companies now have a firewall in place, with 98% investing in anti-virus systems. However, it is not clear whether businesses are simply going through the motions—employing traditional security technologies, such as firewalls—without assessing the risks they face and identifying the key business assets that need protection. Although the use of anti-virus software has risen, for instance, only 53% of firms have implemented intrusion detection measures, and the CBI is concerned that most companies are continuing to rely simply on passwords for access to critical business data. As a result, firms may be leaving themselves open to attack by not having in place appropriate security measures that protect not only themselves but online customers and supply chain partners.

12. Online security is not solely an issue of installing appropriate technology. It is also about changing attitudes and behaviour towards the Internet through education and training. For business, educating employees on security issues can help to secure companies' overall operations and also help employees protect their Internet activities at home. This includes ensuring that security remains up-to-date. Simply implementing technology will not protect online users if the software is not correctly updated—online attacks can evolve to a point where they can evade and elude out-of-date security solutions.

13. However, for many businesses, and particularly SMEs, providing staff training can be costly. The CBI believes the Government should consider providing financial incentives such as tax breaks to encourage and help SME's provide online security education and training for employees. Education and awareness programs, such as Get Safe Online can also make an important contribution to raising understanding of the necessity of implementing Internet security measures. However, as indicated below, more is needed to raise understanding of the collective responsibility online users (from school children to silver surfers) have in protecting their own and others' Internet security.

How much does information security depend on the software and hardware manufactures?

14. As the target, and often victim, of online attacks, companies understand all too well the importance of having security in place to protect their customers as well as themselves. In currently highly competitive market conditions, having effective security has become a key differentiator in the provision of online services, and in being seen as a trusted and secure online provider, partner or brand. Market demand for secure technology solutions is being met by the development of innovative products and tools such as anti-spam filters, anti-intrusion detection software and encryption. Industry solutions, backed by easily accessible, user-friendly and up-to-date advice and support on key security issues and trends, provide users with the confidence that their online activities are secure.

15. However, securing the Internet is not something that can be tackled or solved solely by the software or hardware community or in fact by the business community alone. Businesses, individuals, government and law enforcement agencies all share a collective responsibility to protecting themselves online and addressing

Internet security issues. In February 2006 the CBI launched a joint government-business guide, "Securing Business Value Online", aimed at raising awareness amongst SMEs of the importance of security in their online supply chains. The guide was produced jointly by DTI and a leading group of CBI members, including representatives from both the user and supplier communities.

16. The following are examples of just some of the activities currently underway in the UK and internationally where UK business as a whole is working with government to raise awareness and reduce Internet security threats:

— CBI business guide "Securing Business Value Online: A guide for SMEs in supply chains";
— UK Get Safe Online campaign;
— Internet Watch Foundation (IWF);
— Institute of Information Security Professionals;
— Annual e-Crime Congress Event for business and government representatives;
— Development of CERTs and WARPs in association with NISCC;
— European Network and Internet Security Agency (ENISA);
— UN Internet Governance Forum—addressing spam and Internet security at Athens IGF in October;
— OECD development of a common framework for implementing security and data privacy.

Is the regulatory framework for Internet services adequate?

17. The CBI believes many firms, particularly those outside of London, are still not fully aware of their legal and regulatory requirements when doing business online. As a result, firms may be leaving themselves, and their customers or partners, open to possible regulatory penalties and or legal action. At recent CBI regional workshops, a lack of regional support and information for local firms on the legal and regulatory requirements and security considerations for online business was identified as a concern of many firms. The DTI's work on raising awareness of the importance of information security issues is seen by the CBI as an example of government good practice. Unfortunately, this approach is not being consistently replicated by the Regional Development Agencies (RDAs). The CBI believes the RDAs should be playing a greater and more transparent role in helping businesses understand Internet regulatory issues and in raising awareness of the importance of Internet security. To that end, the CBI believes the Government should investigate the effectiveness of the RDAs in this area, and if necessary devote additional resources. It is vital that regional companies, particularly SMEs, are given consistent levels of support and advice across the country in order to develop their online capabilities and to ensure that the UK continues to grow as a leading market for e-commerce.

18. Internationally, there has been a steady increase in recent years in European and international regulatory and legislative requirements on companies operating online. For many sectors, this can result in a somewhat confusing plethora of requirements. This is a particular burden for companies that share data and provide services to customers and partners across legal jurisdictions. The CBI believes the Government has a responsibility to continue to engage strongly internationally (for example, through the EU and OECD) to ensure UK companies are not negatively effected by changes to international e-commerce legislation, regulation or standards. Financial cutbacks at the DTI do not help in this regard.

Is the legislative framework and criminal law adequate to meet the challenge of cyber crime?

19. If the UK is to reach its full e-potential, it is essential that legislation recognises the ways in which computer networks are attacked and provides appropriate legal powers to deter and to redress business for computer-related crime. The long overdue updating of the Computer Misuse Act (CMA) under the Police and Justice Bill has been welcomed by business, particularly the increase in penalties and fines that will also allow offenders to be extradited to the UK for prosecution. However, to ensure the amended CMA becomes an effective deterrent against cyber criminals, the CBI believes it is also vital that the guidelines for courts on how and when the Act should be applied must also be reviewed. Without this, it is unlikely that the legal penalties imposed will be proportionate to the financial losses suffered by victims of computer crime.

20. As explained above, computer viruses and "botnet" attacks are increasingly being sent via spam emails. The ability to investigate and penalise those responsible for sending spam is therefore an important tool in the fight against computer crime. However, at present the CBI believes the effectiveness of the Information Commissioner's Office (ICO) in combating spam is reduced by inadequate powers and limited scope for

investigation. The CBI has been calling for the Information Commissioner's powers to be reviewed and amended to remove current limitations regarding appeals on enforcement notices and on powers to investigate the origins of spam.

21. Under the Privacy and Electronic Communications (EC Directive) Regulations 2003, if an ICO enforcement notice to cease sending alleged unsolicited direct marketing e-mails (spam) is challenged by the accused, an appeal begins and the notice is effectively suspended. In practical terms, this means spam can continue until the appeal is heard. This can lead to situations where those accused are able to continue their activities, sometimes for up to a year, until the appeal is heard. While the CBI recognises that an appeals process is needed, we believe the ICO should have the power to act quickly and effectively to prevent those accused from continuing to send what is clearly spam even while an appeals process is underway. In addition, the CBI believes that the ICO's information gathering powers should be extended to enable the ICO to require third parties to provide information to track down and identify companies that conceal their identities when sending spam. Currently, the ICO is often prevented from even beginning an investigation as he is unable to identify who to investigate. By addressing these issues, the ICO will be made more effective in implementing the powers given under UK Regulations and help to remove the perception of the UK as an easy target for spammers.

Is the Government equipped to fight Cyber Crime?

22. At a time when the Internet is being heralded as a key platform for the UK's future economic growth and transformation of public service delivery, the Government has a responsibility to place Internet security high on the political agenda. To date, this has been lacking. Of course, important issues such as online child protection have been rightly given high level political attention and support. However, the importance of Internet security to ongoing e-commerce growth in the UK has not been given the sustained, high level political visibility that is needed to bring about change. As mentioned above, the demise of the National High-Tech Crime Unit has been seen as a reduction in the Government's commitment to fighting computer crime. It is understood that the Serious and Organised Crime Unit (SOCA) will be continuing the work of the NHTCU; however, concerns remain at the perceived reduction in dedicated police resources to combat computer crime. Questions remain as to whether the Government has equipped SOCA with adequate resources and the dedicated focus necessary to ensure its work, and the success of NHTCU, can continue.

23. One reason for the perceived lack of Government commitment may be the fact that responsibilities for Internet security within Government are somewhat dispersed between a variety of departments and offices, with little overarching powers of co-ordination meaning that there is, in effect, no government strategy for information security. The Home Office, the DTI, the Cabinet Office's Central Sponsor for Information Assurance (CSIA), and the ICO all have responsibilities for different aspects of information security. While the CBI is not advocating the creation of a single governmental body or agency for Internet security issues, more forcefully co-ordinated co-operation and focus of efforts amongst the departments and offices involved would help. Even, for instance, a single reporting point and clearing house for complaints about spam would be useful for businesses and individuals not expert on what law had been broken (privacy, fraud, etc.) by a particular email—and could help the various agencies decide the best response to take towards the sending party involved.

24. If the Government's vision of the online delivery of public services is to be successfully advanced, co-operation and agreement between departments will be vital. Data sharing between departments is at the very heart of the Transformation Government agenda. Its success will require departments to work closely to develop common polices and procedures that ensure the security, confidentiality and integrity of individuals' data shared, and stored, online.

20 October 2006

Examination of Witnesses

Witnesses: Mr Garreth Griffith, Head of Trust and Safety, eBay UK Ltd, Mr Alasdair McGowan, Head of Public Affairs, eBay UK Ltd, Mr Michael Barrett, Chief Information Security Officer, PayPal, and Mr Jeremy Beale, CBI, examined.

Q566 ***Chairman:*** Let me start by thank you all very much for coming to talk to us. We very much appreciate your giving your time to this hearing and helping us in this inquiry into personal Internet security. Perhaps we could start by you all introducing yourselves and perhaps we could start with you, Mr Beale.
Mr Beale: Certainly. My name is Jeremy Beale. I am Head of e-Business at the CBI.
Mr McGowan: My name is Alasdair McGowan, Head of Public Affairs for eBay UK Ltd.
Mr Griffith: I am Garreth Griffith, Head of Trust and Safety for eBay UK and Ireland.
Mr Barrett: I am Michael Barrett. I am Chief Information Security Officer for PayPal, based in San José, California.

Q567 ***Chairman:*** Would any of you like to make an opening statement or shall we go straight into the questions?
Mr Beale: Straight into the questions, My Lord Chairman.

Q568 ***Chairman:*** Let me start with the first question. The Internet has presented huge opportunities to businesses across the world. It is now clear that it also presents huge security risks to individual users. It is not possible to put a figure, however approximate, on the cost to the global economy of the insecurity experienced by those using the Internet. What are the main categories of cost and where are they borne?
Mr Griffith: The costs that we would experience in this area are around two sites, really: costs to us as a business to try to develop protections for our customers and ourselves. We spend a lot of time and money on resources and tools, et cetera, to protect customers across the world. Then a cost for us personally as a business would be customers who have a bad experience on the Internet generally and turn away from us. I think that is where it gets really difficult to quantify, when you think about lost business. We know that about 17% of active Internet users in the UK have decided not to log on any more to the Internet generally, based on some kind of experience that they have had. That was based on some *Get Safe Online* research that we did. That is probably where the most difficult cost to make out is.

Q569 ***Earl of Erroll:*** Could you just repeat that? Seventeen per cent of those who have used the Internet . . . ?
Mr Griffith: Have said that, through some bad experience or negative experience that they have had, they have decided that they are walking away from the Internet, basically. They do not intend to log back on for any reason—which I think is scary for all of us.
Lord Young of Graffham: That is a very high figure. If people have a bad experience of a shop, they do not avoid shops.
Chairman: Although they might avoid a particular shop, might they not?
Lord Young of Graffham: Yes.

Q570 ***Chairman:*** Has the CBI taken a position on this?
Mr Beale: I would make a number of points. The first is that, when we are talking about insecurity on the Internet, we are talking about a very broad range of things. Information security attacks now are not just of a particular kind; they are of many kinds. So it is hard to quantify an overall figure, precisely because you are looking at very different things involved in that. They often are of an international nature too, as your question indicates you are aware, and there is no systematic collection of data globally of attacks. There is in fact in the UK no rigorous and central collection of information on e-crime as a criminal activity. That is certainly one of the things that I think would be usefully done, because then we could get to grips with this subject in a better way. Precisely because it is not done here, it is not done elsewhere too. It is early days, but it would be a step towards answering your question if it was done in the UK and elsewhere. Having said that, I think that, yes, you see it very much at the company level now—the costs, where they occur—but even for businesses it can be very hard sometimes to ascertain the exact cost of replication, for instance, let alone the assets that might be taken or ruined, or the operational inefficiencies that might have been created.

Q571 ***Lord Harris of Haringey:*** Could I follow that up, My Lord Chairman? You said you think it would be helpful to have statistics collected of e-crime. Do you think that there should be some change in the law so as to define e-crime, so that what would otherwise be a normal crime but because it is committed electronically is then classified in a different way, perhaps attracting different penalties?
Mr Beale: No, I was not thinking of that so much as the police reporting crimes that are electronic, because they are aware. It is usually a crime like fraud, but it might be committed electronically; it

might not be. It might have a component that is electronic. The police would be in the best position to be able to say whether it was really an e-crime or a broader one.

Q572 ***Lord Harris of Haringey:*** So you would look to them to provide the definition?
Mr Beale: Yes. I do not think that a change in the law is particularly helpful in this regard.

Q573 ***Lord Mitchell:*** Do any of you, the commercial companies—eBay and PayPal—have a measure as to the cost of fraud? How many basis points on your business?
Mr McGowan: It is very hard to put a precise cost on it, partly because there is obviously a cost to the individual in terms of losses; there is a cost to business in so far as underwriters' losses. There is also the cost of fraud prevention. We have something like 2,000 people in eBay who are dedicated to trust and safety efforts. They are people who are specifically dedicated to those tasks. I probably would not count within that 2,000, and yet a large part of my job would be dedicated towards trust and safety issues.

Q574 ***Earl of Erroll:*** First, if we improve it, it will reduce employment! On a more serious basis, on that 17%, has anyone looked at how much of that is due to having very unreliable connections to the Internet and so people have got frustrated with using the Internet, and how much of it is actually fear of using the Internet?
Mr Griffith: It was not broken down in that way, but I do think that when you look at the other questions on the survey around relating people's fear of the Internet to things like being mugged on the street, for example, 21% of people rated fear of actually being on the Internet higher than something like being burgled or mugged. So I think it was quite clearly around some kind of negative experience.

Q575 ***Lord O'Neill of Clackmannan:*** Was this a self-selecting sample?
Mr Griffith: It was a *Get Safe Online* survey that was done through—I cannot remember the name of the company—a research agency. It was basically sent out to a random group of active Internet users.

Q576 ***Lord Young of Graffham:*** It was commercial activity on the Internet, not the use of the Internet? In other words, people would still carry on using email but it was a question of going on eBay, or the equivalent.
Mr Griffith: The way it was positioned was that they were walking away from the Internet. It was very high.
Mr McGowan: There is also another issue, which is not just about people switching off the Internet; it is also being less active on the Internet. One of the great strengths of the Internet and of e-commerce is that it has increased the velocity of trade and there is wealth creation associated with that. To the extent that people are less active, therefore, there is probably a cost to UK Plc in that respect.

Q577 ***Chairman:*** Mr Barrett, do you have an idea about what fraction of the monies that PayPal transfers are fraud?
Mr Barrett: We have a publicly published number of 41 basis points, which represents the total fraud costs on the network. Those are costs that PayPal itself bears. That is not broken down in any way and so all classes of fraud are lumped into that. As Garreth noted, however, that does not cover the kind of eBay Inc-level costs for, essentially, the 2,000 or so people that we employ to chase this stuff down.

Q578 ***Chairman:*** Do you have a problem with people thinking they are using PayPal when they are not actually using PayPal?
Mr Barrett: We have a serious problem with it. It is precisely the kind of incident that victimises both our brand and us as a company, as well as them as consumers and their experience of it. So we want to do whatever we can to prevent that from occurring.

Q579 ***Lord Mitchell:*** This may be a ridiculous question, but is there any impersonation of eBay at all?
Mr Griffith: Yes, we have a similar problem.
Chairman: They are all over the place. I think there are more impersonations than there is eBay!
Lord Young of Graffham: I am not sure.

Q580 ***Chairman:*** That is an issue. I cannot remember whether it comes up in the questions, but are you heavily involved in prosecutions over your own logos? The incorrect use of your own logo?
Mr Barrett: Typically speaking, we find it more useful to prosecute these criminals for straightforward fraud rather than to go after them for IP infringement.
Chairman: Let us get back to our questions. Lord Young?

Q581 ***Lord Young of Graffham:*** Our inquiry here is really concerned with personal Internet security. Who do you think should take responsibility for it?
Mr Griffith: In my opinion, it is a broad range. I think that we all need to take responsibility for it. By that I mean law enforcement, the Government, industry, as well as the individual. I often liken it to offline analogies of driving a car, where the car

manufacturer has responsibility; the people who make the roads have responsibility; law enforcement have responsibility; and the individual behind the wheel also has responsibility. I guess we would be maybe likened to the car manufacturer or even maybe the council, taking care of the roads. However, if it has a seat belt in it but no one knows how to use the seat belt or what it does, it is ineffective. I really believe it is across the board. We strongly believe in partnerships. We work closely with rights owners, with law enforcement around the world globally, with people in the Government. You name it, we work very closely with people. I cannot believe that just one entity, standing alone, can make a significant impact. I think that it is all about partnership. That is why we are heavily involved in *Get Safe Online*. We saw that as a great way to initiate that partnership with government, law enforcement and industry, to start trying to make a difference on education as well as other things.

Q582 ***Lord Young of Graffham:*** Partnership is no consolation if I have just lost something as a user and I cannot distinguish, or will not distinguish, between the software vendor, the hardware vendor, the ISP or eBay—whoever it is. In some instances it might be my fault, but how do we distinguish between that and liabilities? Who between you all is going to come to me and say, "We will recompense you for the loss you have suffered"?
Mr Barrett: At least on the PayPal side, if the customer's PayPal account was tapped into illegally then we make the consumer whole. So they bear no financial cost, and that goes into the 41 basis points that I talked about earlier. The issue is simply that for too many of them the experience is so wholly repugnant, and it is kind of like being burgled, that they do not want to have anything to do with the Internet again—and I am not sure whether you can entirely blame them.

Q583 ***Lord Young of Graffham:*** So that is really something which is going to hold back the development of the Net altogether.
Mr Barrett: That is one reason it is such a strategic priority for us to address this issue.

Q584 ***Lord Mitchell:*** Can I just come back to your survey very quickly? Was this UK or was it international?
Mr Griffith: UK.

Q585 ***Lord Mitchell:*** Is it possible to get hold of a copy of that?
Mr Griffith: I was going to say, we would be very happy to send you one. That would not be a problem at all.

Q586 ***Lord Young of Graffham:*** Finally on this, are you in favour of holding software vendors responsible for flaws in their security?
Mr Griffith: Yes, I think so.

Q587 ***Lord Young of Graffham:*** There is a lot of implication about development of software and everything else, if you are going to hold them responsible.
Mr Griffith: It is a difficult question, because I do believe responsibility sits squarely across the board. So who is responsible for helping the user to understand what the software is about, how to install it and how to use it? Then who is responsible for them making different choices when an email comes in on whether to click on that link or not? I do believe that we are all responsible. I think that we take a lot of responsibility at eBay for the behaviour of our users and whether or not we have educated them or empowered them with tools. I do not want to speak for the software manufacturers, but I would say that if I were them I would want to take responsibility for the flaws in their system.
Mr McGowan: I think that there is one other issue here. That is the role of education in educating consumers about the need to update software continually. That is part of what *Get Safe Online* is about: educating consumers, so they know it is not enough just to buy an anti-virus software, a firewall, install it, and then everything will be fine; because the fraudsters and the hackers out there will always be trying to find new ways of breaking through the systems.
Mr Barrett: I think that one of the thorny issues in this particular field if one talks about software vendor liability is what is the statute of limitations on that, effectively. Picking on Microsoft—because everybody likes to!—you get this issue of, "Okay, there's Windows 98 and Windows ME, and so on", so where should they be no longer held liable for software flaws in that software? Despite the fact that we still have $1\frac{1}{2}\%$ or so of our customers using Windows 98, despite the fact that it is now close to a decade old, it is completely out of support, and potentially quite dangerous for them to be doing that. One of the things we try to do is essentially to nudge our customers on to more modern and safer operating systems and browsers, but we cannot, in the final analysis, actually force them to do so.
Mr Griffith: I think that there is something around "reasonable endeavours". I would hold all companies responsible that they are reasonably doing everything they can.
Lord Young of Graffham: But it is no consolation to me that all companies are responsible; I need someone specific to go for. This is where the difficulty really comes. It might be that overall everybody

should work better together, but that is not the way the world works. There is a point. If it is a software flaw and somebody breaks in—a phishing exercise or whatever—and I lose my PayPal account and I lose my eBay account, it is not my responsibility. Unfortunately, it is not really your responsibility but it is your liability. That is where we are at the moment.

Q588 ***Earl of Erroll:*** Surely Windows 98 is fairly safe now, because no one bothers to attack it any more? The real problem is, if I go into an eBay site or a PayPal site, how do I know that that is PayPal or eBay? Surely you should be authenticating yourselves back to the user, possibly through a second channel and not through the same line as they have come in, in order to make sure it is absolutely secure? So to a large extent the software we are talking about, and the people who perhaps are producing the defective software, are yourselves.
Mr Barrett: There was an initiative that came out recently, which goes by the incredibly dull name of "extended verification SSL certificates". Essentially, what it does is, when a website communicates to a web browser, it uses this secure socket layer, encrypted session.

Q589 ***Earl of Erroll:*** In other words, IE7.
Mr Barrett: Exactly right. So as part of Internet Explorer 7 there was support built in that, if a website is using an extended verification certificate, their URL address bar will glow green. We were very keen when that facility was enabled in Internet Explorer that both PayPal and eBay sites should be fully enabled for that. That was launched about two weeks ago and we were indeed one of a decent number of e-commerce sites that was already enabled for that. It is also worth noting that 30% of consumers are now using Internet Explorer 7. So there is actually a fairly good fraction of consumers that now can tell very straightforwardly whether they are in fact on the legitimate PayPal and eBay websites.

Q590 ***Earl of Erroll:*** Can I say that, unfortunately, Parliament is not—because of other issues in the system? There must be quite a lot of other corporates, because there are incompatibilities, I believe, with other components in the system. Also, for instance, IE7 will not communicate with the Thomson SpeedTouch router; you have still to use IE6. Until people are upgraded across the board, you cannot necessarily rely on the latest technology—as you have already said—being deployed. So should we be looking at things which are technology-independent?
Mr Griffith: I have one addition to what Michael was saying. We have had our toolbar—what we call our eBay Toolbar with Account Guard—for about four or five years now, which is downloadable onto any version of Internet Explorer. It effectively does what Internet Explorer 7 now does, and has done for a few years now, namely if you are on a site that is not eBay or PayPal, you basically get a pop-up; it flashes red, and there is no way of missing that you are not on it. The simple way to look at it is, if it does not go green you are not on eBay or PayPal. Fundamentally, it turns green if you are on our site. If you are on any other site on the Internet—Microsoft, Amazon—it does not. We have had that for a while. On the email front we have this address spoof@eBay.com or spoof@PayPal.com, and if you send any email to that address and just wait a few minutes, we will tell you whether it is real or not. So we have pretty robust ways of helping you know if you are on the right site or if the email is rigged.
Mr McGowan: And it is free to download.
Earl of Erroll: I think that you should publicise that email facility better, because I certainly know my wife does not know about it.

Q591 ***Chairman:*** Does that operate on FireFox as well?
Mr Griffith: The toolbar does now. A while ago it was not, but now it is functional on FireFox.

Q592 ***Chairman:*** Mr Beale, can I ask you what the CBI position is on holding software companies liable for faults in security in their software?
Mr Beale: The simple answer is that we do not have a formal position; but, to give you something a bit more informative, we hold the view—as the other speakers have today—that this is a mutual responsibility amongst a number of different actors. Having said that, I also take Lord Young's point that if everyone has a responsibility no one in particular has the responsibility. I think what needs to be done is a much clearer working-out of where responsibility lies for different actions along the chain of supply, according to what one's capabilities are in that chain of supply. This has never been systematically done, and I think it would be helpful. I should add that there are also existing laws that cover liability, neglect, et cetera, which are probably quite adequate in many cases. So I am not advocating some great new legal framework for this. I think—and this will underline a point that I will make a number of times in terms of the questions that I have had presented to me—that what is really needed is, as we term it, a national information security strategy. By that we mean an educational programme that is given high priority; that is linked to a training programme; that is also linked to an improvement in enforcement capabilities. So a significant national campaign, but part of that would be the development of a better understanding of what different groups, including

software groups, can and cannot do in terms of providing security, and of course including individuals.

Q593 ***Lord Mitchell:*** The CBI evidence says that companies are leaving themselves open to attack by failing to implement adequate security measures. What should be done about it? Could I add, would you prefer to see these problems being addressed by regulation or by the creation of efficient incentives, or should companies simply be left to get on with it?
Mr Beale: What I have just said was a bit of a prelude to this question. The point about many companies is that they are not aware exactly of the kind of threats they face, and so are not necessarily able to evaluate what they need to do. Many large companies have that capability. Even they often do not get it right, but particularly small and medium-sized companies do not have access to the expertise necessarily, or easily or cheaply, to be able to properly secure themselves. There is also the fact that of course the threat is constantly changing. As we are probably all too aware, every time you think you have defended yourself against something, another threat appears. So I think there is a major issue here. This is why I think we need a national information security strategy to deal with that. Having said that, there is also the problem, as I have just mentioned, that technical resources are often expensive. There are not that many people available widely across the economy who can provide the expertise that will necessarily help companies, and so we need a lot more effort going into the development of that expertise. Again, large companies can afford to pay high salaries to people who are very good at information security; but it is often out of reach of small and medium-sized companies who cannot do it on an ongoing basis—and yet an ongoing basis is exactly what may be required. To come back to your second question, if you establish a regulation the only trouble is that you establish it in relation to a specific set of technologies. If the technologies change with another kind of threat, the regulation is irrelevant. Rather than trying to find a silver bullet, *a* regulation or *a* set of actors that can solely resolve this problem, we need a much greater combined effort, led by government, that will help raise awareness, help develop expertise, across the UK.

Q594 ***Lord Mitchell:*** Do you think companies should be held liable if their systems are inadequate?
Mr Beale: I think the answer given a bit earlier was quite good, about "best endeavours"; but, again, I go to the point that it is often very hard for companies to know what they are meant to be defending themselves against. Again, to say, "You have total responsibility for having been unprepared" can seem a bit disproportionate at times. When they are clearly being negligent, that would be a different matter.

Q595 ***Earl of Erroll:*** Would you like to see a security breach notification law in the UK, like there is in some of the United States?
Mr Barrett: This is an interesting question. I think that you can look at what has happened in the United States as that it has fairly effectively shone a light on to what you could describe as inadequate data custody practices; but it actually is not very helpful from a consumer perspective. If you get a letter in the mail—as I did recently myself—you look at it and say, "Okay, what am I supposed to do with that and what does it tell me about my own personal risk?". It is also very much an exercise in shutting the stable door after the proverbial horse has bolted, because a company that experiences one of those breach notification moments almost always then implements a much stronger information security programme than they had before the notification moment. The question is whether we would all be better served with uniform data custody standards. I think that is quite a difficult thing to pull off from a legislative perspective, because you also run into this problem that you do not necessarily want to enshrine in primary legislation what amount to a series of technical standards. It is then the question of how you actually set a good baseline standard, in a way that does not mandate specific technologies.

Q596 ***Earl of Erroll:*** In which case, what you have said is, though there is an element of shutting the stable door after the horse has bolted, actually it has given the motivation to do exactly what you wanted—and which you have just said legislation would not do. Therefore, it is working in that they are, even if retrospectively, upgrading their data security standards.
Mr Barrett: I would argue that you can achieve the same effect by enabling data custody standards. In fact, in the United States the payment card industry standards, or PCI, has been fairly effective at helping the credit card community in getting its information security posture something closer to the right level. That was not mandated by the Government; that was simply mandated by the credit card networks.

Q597 ***Earl of Erroll:*** The problem is that they are in the business of handling money; a lot of the data thefts are actually from systems that are not, such as social security systems and traders, and people like that. One of the points made earlier is that this also means that it is reported to the authorities, so one has a handle on how big the problem is, and this would not be reported if it was not for these data breach

laws. Would there be a purpose in keeping them so that we actually know the scale of the problem?
Mr Barrett: In theory, that makes sense. I think the devil is in the details, to be quite honest, when you are discussing at this level of abstraction. You have to get a bit closer to how any proposed scheme might be implemented. In principle, I see no issue—and this is me speaking personally rather than any formal corporate position. I have never personally had a concern about the notification requirement *per se*; it is simply that it does not actually fix the behaviour that you want to change, which is stronger data custody.

Q598 ***Earl of Erroll:*** Do the CBI have a view on this?
Mr Beale: No, we do not have a formal position. We do see that having a system so that everyone understands where they stand could be useful. The reports that we get from members about the US situation is that it was introduced by politicians wanting to have a quick fix to what is clearly a problem; but that the requirement is disproportionate to the actual threat and, as a result, it is extremely costly. If anything like this were to be introduced, it would be good if it was well developed, after a lot of discussion with the various industries about what it would entail and, as I have said, as part of a broader effort to develop understanding of what was actually involved.

Q599 ***Earl of Erroll:*** In other words, no mass mailings out to customers. Use it more intelligently.
Mr Beale: A more focused view, yes.

Q600 ***Lord O'Neill of Clackmannan:*** Mr Barrett, you have made the point several times that it is 41 basis points. Is that a figure which has been changing, given increased volumes?
Mr Barrett: It does move. I have only been with PayPal just over nine months myself, so I am not sure I could tell you with any great accuracy the long-term historical trend line. To a very large extent it is driven by the effectiveness of our back-end fraud control models. What will happen typically is, if there is some kind of temporary spike in fraud, then we will tune the fraud protection models and that will drive it back down again. As far as I know—but, as I say, I do not have enough longevity with the company to tell—it does just bump around in a certain range.

Q601 ***Lord O'Neill of Clackmannan:*** This is for anyone who wants to answer. Are the police able and willing to investigate fraud or other criminal activity online? What has been your experience of dealing with the police in these matters?
Mr Beale: I can speak generally, but maybe others have direct experience.
Mr Griffith: We work very closely with the police. We have two distinct groups within our trust and safety teams: our law enforcement relationship management team and our fraud investigation team. One is more proactive. We are basically reaching out to law enforcement and helping them to understand the issues on the Internet, for example, and over the last couple of years we have trained 3,500 police officers. We either go out to them or they come to us. About 100 at a time come to us, either in Dublin or in Richmond, and we go through a training process. We find that the willingness at a personal level is there. When you speak to a police officer, they are dying to be there, to help out the people in their community, et cetera, and investigate. Their challenges often are the tools that are made available to them and the priorities that have been set for them. We find them being quite frustrated, especially at the local level. In a local police station, for example, some of them are not able to access the Internet. When someone comes in and says, "I got this item on eBay. I'd like you to take a look at it", they cannot actually go and take a look at it. There are some fundamental things like that which cause a real challenge for police officers, and I hear a lot about that. One thing, which is maybe one step higher, is that I have found the priorities are generally around higher-value issues. What happens on eBay tends to be lower-value, higher-volume types of things. When we try to get police engaged, sometimes they say, "Look, we'd love to help you. If it is not over 'x' threshold"—thousands of pounds, or whatever it is -- "we can't help you". The other thing is that, if it is a criminal issue—we are not a criminal agency and obviously we cannot take action against people—we do have a very streamlined process, where we work with law enforcement if they come to us. We ask our community of users to go to their local police stations, get them to contact us—and we give them numbers, email addresses and everything they need to contact us—and then we can work with the police. What we find is the users coming back to us, saying, "They're not interested". It is only a £500 laptop, or whatever the issue might be. So I think that we see frustration on both sides. We see law enforcement being frustrated because they want to engage, but either they cannot technically or prioritisation-wise, and we see users saying, "We're trying to knock on their door and get them to listen, but they can't help".

Q602 ***Lord O'Neill of Clackmannan:*** Do you monitor this across countries? Obviously you are an international organisation. What is the experience, let us say, within the EU? How does the UK stand up to comparison with other police forces in other jurisdictions?

Mr Griffith: In my experience I would say that it varies by different countries. There does seem to be a general issue around scale. The issues we see here seem to be very similar across Europe. I would say that in many of the countries it is probably an even more significant challenge for law enforcement. That being said, when you do have something of scale that crosses the threshold into a number volume or a monetary volume that is relevant, we have great working relationships. Someone mentioned earlier about the spoof, the phishing guys. A lot of our challenge comes out of Romania actually, out of Eastern Europe, and we were recently involved in an arrest of five people in an Internet café, where us and the United States' secret service went in with local law enforcement and managed to catch these guys sending out millions and millions of emails. So when you are talking in big-scale volumes, you start to get some help; when you are talking at the lower levels, which most of our users encounter, it is a bit difficult.
Mr Barrett: Perhaps I could add to that. Definitely on a global level the threshold problem is a serious one. You will often find a case where it may be that the threshold is, say, $50,000 or something of that nature before you can get a prosecutor interested in a case. So, as we compensate our consumers who have been victimised, we are running the meter up and slowly building up a dossier on some particular individual, until such time as, "Aha, we are now over the threshold!". But if it was 50, and it is in some cases, and we first found out about this guy when he had stolen just $1,000, that is 49 more cases at $1,000 each before we can get him arrested. So I think you can argue that the threshold problem is causing the public real harm.
Mr Beale: We have quite a few reports from members that they feel that the technical competence of the police nationally, across the board, is not as high as they would like and need to deal with these. Centrally that expertise might exist, but in a number of local forces it does not exist, and that is obviously where the problem lies, because that is where people are meant to report at the moment.

Q603 ***Lord O'Neill of Clackmannan:*** That would be the reason why your evidence suggests that a number of your member companies are reluctant to report cases to the police, or is it a recognition of the threshold issue as well?
Mr Beale: It is both, and it is reputational too: that they do not always want to advertise when they have had a problem, I should add. It goes back to the point about resources. The police obviously have limited resources to develop this expertise. There is a limited supply of people with these capabilities, and it is a general problem that not enough people are coming out of universities with IT skills. I do not think that information security is yet a required part of getting an IT qualification. I may be incorrect about that, but a lot of effort has not yet been put into developing this capability nationally.

Q604 ***Lord O'Neill of Clackmannan:*** Do you think that the activities which are considered criminal are covered by the law, and therefore people would be willing to report to the police in order that action could be taken? Do you think that the law is clear enough in its definition of what is criminal in relation to e-theft?
Mr McGowan: I think certainly the new Fraud Act will help. The Computer Misuse Act amendments which went through the Police and Justice Act will also help. Again, it ultimately boils down to enforcement. Also, there is a broader issue here in terms of how you tackle this on a cross-jurisdictional basis. Ultimately, the legal framework is only as strong as the weakest link in the chain. So if others' jurisdictions have weaker protections in place, then you will simply see organised gangs migrating to those jurisdictions. There has to be international co-operation at a governmental level in that sense.

Q605 ***Lord O'Neill of Clackmannan:*** One last question on the issue of the quality of policing. We have had evidence which suggests that, once the police have become good at detecting, you guys recruit them as security officers! Apart from that side of the equation, could you put a figure on what you would consider to be a reasonable amount of money or resource that the police should be putting on to this issue? Are you happy that they have enough people involved in it? It would appear that in some areas you say that there is not. I am not asking you to pluck a figure out of the air, but do you have any idea of how much more could be done by the police to encourage you?
Mr McGowan: I think it is very hard to put a precise figure on it. To pick up your point about recruiting ex-policemen, we plead guilty in that respect, in so far as our head of law enforcement relationship management is an ex-Scotland Yard detective of 30 years' standing! On the plus side, however, his role is, as Garreth says, to go out and train the police, and also trading standards, as to how they can work with eBay and with PayPal to deal with the problem. I think that we are very conscious that there are only limited resources available to the police. Clearly it is a matter for the Home Office and the police to determine national policing priorities. Perhaps one thing we would urge is that, when they are deciding their priorities, they take into account the threshold issue and, in assessing harm, focus on the high-volume but low individual loss cases. So if they have a clearer sense of the overall picture and therefore of

the overall harm that is being created by phishing attacks, that may possibly input into some of the national policing priorities.

Q606 ***Lord Howie of Troon:*** Thinking about this threshold you keep talking about, is there a national threshold or is the threshold invented by each particular police station?
Mr Griffith: I would say that different police stations have different thresholds. I cannot give you a number. I have not encountered it as, "Oh, there's the cross-over", but it does seem to be on a case-by-case or station-by-station basis. So I imagine that it is depending upon their resources.

Q607 ***Lord Howie of Troon:*** Does it vary quite widely?
Mr Griffith: Again, I am not sure. I would say that it probably does not vary a lot.

Q608 ***Earl of Erroll:*** On this aggregation of cases and threshold, you are telling us that it is too small—say £500, £1,000, whatever it is—to report to the local station, and hoping they will come back to you. Could you not aggregate all these cases, work out if there is a single person behind it, then present the entire dossier and then, at that point, say who had been defrauded?
Mr Barrett: We do it. We precisely operate that way.

Q609 ***Earl of Erroll:*** I just wanted to clarify that that is what you can do.
Mr Griffith: We do that. It is in cases where maybe we have not done it on that particular criminal perpetrator, or whatever it is—but we do that, yes.

Q610 ***Lord Harris of Haringey:*** Can I switch to spam? Do you think UK laws on spam are fit for purpose—to use a popular phrase?
Mr McGowan: I know that there have been issues raised about the investigation powers of the Information Commissioner and issues to do with the appeals process for the Information Commissioner. I know others have commented in the past that there are issues about penalties with the UK spam laws. I would come back to my earlier point that enforcement of the law matters too, and if other jurisdictions have weak spam laws then, ultimately, people will migrate to those jurisdictions. So I think that one has to look at it on an international basis as well as a national basis. I do not know if Jeremy wants to comment further.
Mr Beale: I would agree, but I do not think that there are any more laws or legal powers; it is the actual getting the ability to implement those. As I understand from the Information Commissioner, they are not calling for any more formal powers under the law; they are just asking to be given explicitly the ability to do what they have been asked to do. The prosecutions for spam in this country—or the lack of, compared to some other countries that operate under the same European directive, where there have been more prosecutions—indicates that there is something of an issue here.

Q611 ***Lord Harris of Haringey:*** Specifically in your CBI evidence you make the point about the notice being suspended if somebody commences an appeal. Is that derived from the EU directive itself or is that a UK variant?
Mr Beale: I am not a lawyer, so I have an inability to be able to say specifically the fault in that, but we understood that the DTI would be able to enable the Commissioner to get greater capabilities in that regard. We also understood, I think it was last summer, that they had started a review of this; but we have heard nothing further.

Q612 ***Lord Harris of Haringey:*** But the CBI would in principle be happy with the idea that enforcement action should not be suspended if somebody lodges an appeal—because clearly that could have ramifications in all sorts of other areas.
Mr Beale: This is where the lawyers come in, because it depends on the nature. If it is clearly spam, then definitely; but there are cases of "Is it spam? Is it not?", which is where at the moment the Commissioner cannot do anything—and that does not seem to be right. The reason—and I am not just trying to split hairs with you here—is that we think an effective mechanism that everyone understands would be better than one where everyone is clearly fairly dissatisfied with it. We are not greatly in favour of onerous powers of inspection or the ability of the Information Commissioner to arbitrarily close down websites, or anything like that—or at all, of course. However, we are also saying that at the moment there is a situation in the UK where there is a lot of frustration with the situation over spam, and so it would be helpful if there was more clarity to enforce the law.

Q613 ***Lord Harris of Haringey:*** Mr McGowan is clearly itching to say something!
Mr McGowan: I know that there have also been issues around whether it should apply to business email accounts, and there has been some frustration there in the past. Although phishing is just one subset of spam, and there is another part of spam which is just nuisance and clogs up people's in-boxes, but to tackle the phishing part—which generates fraud and creates damage—there the Fraud Act will help, because that creates a new offence of "fraud by misrepresentation"; but that still comes back to the

point about enforcement. It is important to think too about technological solutions and how you keep it simple for the end-user. We have on eBay a system called "My Messages", which is essentially a web-based, dedicated, personalised in-box which somebody has. We therefore have a simple message which we can give to our users that if a message is in "My Messages", i.e. their in-box that they have on eBay, then they can be sure that it is from eBay. If it is not, then they cannot be sure. That keeps it simple for people. Mike may want to talk about the safety bar that has been introduced by PayPal, which directs spam messages to people's spam folders.

Mr Barrett: There was some talk a couple of years ago that digitally signing emails was going to be the ultimate solution to spam and that, after that occurred, the problem would largely be solved. Unfortunately, what occurred then was the predictable IT industry standards fight, with various factions disagreeing with each other as to what the technology should look like. Those standards, because there were multiple of them, did not go anywhere. Subsequently, what PayPal and eBay have done is that we are now in a position where we are 100% signing all of our outbound email—which does not sound terribly interesting, except that what it then allows us to do is to work with the top half-dozen ISPs. If you look at the distribution of email addresses across ISPs, it is one of the classic, very long-tailed curves; but the first six ISPs, which are all of the ones you would expect—like Yahoo, MSN, Hotmail, Gmail, and so on—represent 50% of the email addresses on the planet. So what we are trying to do is to work with those ISPs and get them to drop anything that says it comes from PayPal or eBay but in fact is not properly signed. That will start to have impact before the end of this year, as we work with those ISPs.

Q614 ***Lord Harris of Haringey:*** At one stage business lobbied for exemptions for unsolicited business-to-business email. Is that still the position of business, or do you no longer feel that is appropriate?

Mr Beale: We have not formulated a specific position there. I can describe the broad situation. We get a lot of businesses complaining about the amount of unsolicited emails they get. Some of them have even gone so far as to say they are going to deny their staff email, so that they will not be distracted by this; they will not clog up their services, et cetera—which is an unfortunate situation, obviously. On the other hand, there is amongst businesses, compared to individuals, a greater desire to be able to be informed about what potential suppliers may be able to offer them and to know about what is going on in the market. So I do not think it is an either/or situation. It is certainly a lot more ambiguous than in relation to unsolicited emails to individuals.

Q615 ***Lord Harris of Haringey:*** There have been various examples of reputable companies farming out email marketing campaigns to other, perhaps less reputable, companies who, in turn, send email spam to individuals who have never asked to receive it. I think that Sainsbury's mobiles and Virgin wines have been caught out, and there are reports of T-Mobile using a quite unsuitable list of email addresses which was bought off eBay for £20. Do you see this being a problem that can be stamped out—and, if so, how?

Mr McGowan: I do not know the specific case you are referring to in respect of eBay, although it sounds like the sort of listing which we would probably end. We are pretty clear in our privacy policy that we do not share or rent or sell personally identifiable information to third parties for their marketing purposes without members' explicit consent.

Q616 ***Lord Harris of Haringey:*** If somebody advertised something on eBay saying, "We've got some good address lists for sale", you would not allow that?

Mr Griffith: No, we would not allow that. We would take it down.

Q617 ***Lord Harris of Haringey:*** More generally, do you think there are things that would enable the problem of this being farmed out to less reputable companies, who then do things that perhaps are deniable by the main company?

Mr Beale: In general, I think that good, reputable companies try to, and should, develop codes of conduct internally for how they deal with data. They obviously have requirements in terms of how they deal with personal data but, more general data, they would and should develop those according to their own individual business situations. I think it would be very hard—if this is where you are trying to get—to formulate a law saying how they should handle general data that they hold in relation to their suppliers. You might end up actually restricting the operations of supply chains.

Mr Barrett: Perhaps I may answer a slightly different question from the one you in fact asked. I was talking with Bruce this morning about spam generally, and I confess that I get slightly irritated when people say that spam is an unsolvable problem. Personally speaking, I have had the same email address for nearly a decade and, when I have my spam filter switched on properly, I see essentially no spam. I get probably one piece a week or something of that nature, and I get a perfectly acceptable false-positive rate where something gets mis-categorised as spam. You can always argue, "Yes, that's an arms race",

and so on—and, yes, it is. On the other hand, the difficulty we are dealing with is the fact that those technologies have by and large not been put in front of consumers. The obvious piece of the overall ecosystem that represents the Internet that could do that are the ISPs. One of the questions is why have not the ISPs done more to protect their consumers?
Lord Harris of Haringey: Not the question I asked, but an interesting answer!

Q618 ***Lord Howie of Troon:*** Is there any difference between buying and selling email addresses and buying and selling ordinary postal addresses, which has been going on for many years? Membership lists and things.
Mr Griffith: I suppose no. It seems to me that I do not want my address being sold out there, if I am not willing to be contacted at that address. That is the difficult challenge. People are talking about "offline spam", which is that stuff that makes its way through our door. In most cases it does not have my address on it. It is just someone walking round the street, sticking them in the boxes—which is slightly different, I suppose, to the challenge on the Internet. If you give out that email address, that is my way into your door. So it is slightly different. I am not sure of the right answer to that question.

Q619 ***Lord Howie of Troon:*** It is an answer anyway.
Mr Beale: I am not quite sure where this is going, because there are obviously legal restrictions on what companies can sell to other companies in terms of personal data about individuals. That is under the—what is it called?

Q620 ***Lord Harris of Haringey:*** Data Protection Act.
Mr Beale: Data Protection Act, thank you. A post code is not individualised.

Q621 ***Lord Howie of Troon:*** Mine is actually.
Mr Beale: It is usually down to about a road, but it is rarely to one building and one individual within a building. An email address, of course, very often is to an individual. So I think that there would be a difference. You can get a general email account for a company, which would be different. One other point is that the DTI did initiate internally a review of business-to-business unsolicited email—which is probably a more useful term than "spam"—to see if there was further regulation or anything more that needed to be done in this area. Again, I have not heard if that has been concluded or any outcome that has come from that.

Q622 ***Lord Howie of Troon:*** It just strikes me that membership lists of learned societies, and so on, have been bought and sold for years, like postal addresses. I think that this is a distinction without a difference.
Mr Griffith: I think that it does come to what Mike has said. The equivalent of the spam filters is having channels below your post box, through your door. It channels it that way into your bin, or it channels it that way into your in-box. I have had an email account with Yahoo for about 15 years and I get no spam. My spam in-box fills up quickly, but I never go look at it. My in-box is pretty clean every time. Frankly, with Yahoo they just turned it on for me, which I have found very helpful. I can opt out, but they turned it on for me. It is something that increasingly we need to do as an industry: to be a bit more—"parental" maybe is not the best word—but guiding our users and maybe trying to help them out by turning something on for them. Microsoft's Internet Explorer 7 anti-phishing functionality is actually defaulted off—which is surprising. You have to turn it on yourself. I was thankful for Yahoo for turning on my spam filter, and that is something we can do as a business. It effectively removes the problem from our users' in-box.

Q623 ***Chairman:*** Is this not something, Mr Beale, that you think business should do? Here we have had two suggestions. Mr Barrett was saying that ISPs should be required to turn on these sorts of filters, and perhaps the browser-makers should also be required to have this as the default setting.
Mr Beale: I understand the desire. I am sure that there are things that can be done, and I know that there are things that are being done. These companies are doing things themselves and some ISPs are doing things. Is it ISPA or Lynx that has developed a code of conduct too for its members? I also think that the ISPs cannot solve all the problems. It is sometimes very hard for them to track where emails are coming from. If it is a botnet, for instance, they do not know that the person whose machine it is coming from is the person who has launched the attack. If they try closing it down or blocking emails from that person, they might have a legal problem there in terms of their contractual relations. This is why I was saying that trying to identify a silver bullet for all problems is not very workable. It is also why I was saying that it would be useful to develop a dialogue with the groups that are working on this, to identify what they can do and are doing. It would be very useful.

Q624 ***Lord Patel:*** Are there companies failing to meet their legal obligations when doing business online?

Mr Beale: I saw this question. I think we said they were not necessarily aware of all their legal obligations necessarily.

Q625 ***Lord Patel:*** Weasel words!
Mr Beale: I want to explain why I did not mean it in quite that weaselly way. Precisely because a lot of the online activities, as we were just discussing, are actually covered by existing laws, but do so in new ways, companies may not be aware. I am really thinking of SMEs here. They might not have the expertise to know how a fraud is committed online, such that they need to develop a specific risk management strategy for dealing with that. Also, a lot of them that we hear about feel there is a problem out there. They are very aware, they read in the press lots of reports, and they are afraid of getting into difficulties; but, again, they do not know exactly what they need to do.

Q626 ***Lord Patel:*** Are you saying that there are companies who do not know their legal obligations when doing business?
Mr Beale: In relation to e-crime, yes.

Q627 ***Lord Patel:*** So what does the CBI do to inform them?
Mr Beale: We have done a number of things. We have ongoing activities in this area with our members. We launched—as we cited in our evidence that we submitted—a guide for SMEs and their supply chain partners, because obviously in some respects it might not be you that is doing something wrong but a partner that you have engaged in business with, which then creates a problem for you. We did that with DTI and Ernst & Young. Frankly, we have limited resources, have a limited voice with the business community, and this is why we say that a much larger-scale, higher-profile campaign led by the Government would help in this regard, so that they were hearing about the problems; they were being informed about where expertise that could help them lay; and where there was increasing devotion of resources to the development of that expertise. I think that could help turn round the problem quite significantly with the broad mass of businesses in this country.

Q628 ***Lord Patel:*** You do not think some high-profile prosecutions might bring it about?
Mr Beale: I was interested in that question. It would certainly momentarily raise some interest, and everyone would probably think, "Oi! I hope that isn't going to happen to me. I had better have a look". Just to take—without in any way wanting to pick on them—Nationwide, which is pretty high profile, they did get hit with a significant fine in this regard. I will point out that Nationwide is in an area that is already heavily regulated; where there are many rules in place; where in many respects they are probably a very knowledgeable company; and if even they have a problem, you can imagine what it is like for companies who do not have those resources.

Q629 ***Lord Patel:*** That was about losing their information. It was not necessarily not fulfilling their legal obligation when doing business.
Mr Beale: I was reading the FSA's report on the case on the way over here, just to make sure I was familiar with it. As I understand it, Nationwide was found not to have complied with the principles laid down by the FSA. What I am saying is that we have had a pretty big case there, where the company—despite its best intentions, despite being in a very heavily regulated area—still managed not to do all that it needed to and, once it found out, did do it. However, I do not think that will change the massive problem that we face, which is that many, many companies do not have the ability to know what to do.

Q630 ***Lord Patel:*** So you would agree that the CBI calling for more education at a regional level is not going to achieve much?
Mr Beale: This is why I have said a national campaign is really what is required, but that would be very much in the regions, because that is where a lot of the SMEs, and certainly a lot of our smaller members, tend to be located. That is also where—as we were talking about earlier—there is this variable quality in terms of the provision of the ability of the police forces to follow up.

Q631 ***Lord Patel:*** Who should lead the national campaign?
Mr Beale: As I said, I think that it should be a Government-led campaign, by which I mean that the Government should take a lead role; but it should be one that is done in close co-operation and co-ordination with those private sector groups that have expertise and knowledge and that are active in this area. It really can only come through a partnership of business and government; but if the Government at the highest level did lead this, it would be helpful in that regard. I should also say that I think there is an opportunity here. The Conservative Party has called for the creation of a homeland security agency, along the lines that exists in the United States. The Chancellor has called for a national security strategy to deal with the threats, including online threats, that the UK faces. We would see a national information security strategy as one part of that. If it could be explicitly defined as such, that would help it. Precisely because information security is often seen as part of the problem for companies, it is seen as a technical

issue—a techie issue for the geeks—when in many respects it is actually part of an overall security strategy that companies have, and it is the same for the UK as a whole. It needs to be seen not as somehow separate from security in general but as an essential part of it.

Q632 ***Earl of Erroll:*** I just want to clarify a couple of things. I know that we talked about the phishing problem earlier, but there are a couple points on top of that. At the moment, the banks refund phishing losses. Do you do the same?
Mr Barrett: Yes, we do.
Mr Griffith: For consumers, absolutely we do.

Q633 ***Earl of Erroll:*** You have been talking about issuing a low-cost security token. That will protect against password-stealing attacks okay, but it will not protect against some of the man-in-the-middle attacks. Do you think that you could be leading people into a false sense of security? Earlier, I referred to the two channels for authentication of who is using a mobile.
Mr Barrett: By an odd coincidence, I actually brought mine. You can look at it later, if you like. It just displays a rolling six-digit PIN that changes every 30 seconds. The answer is that while these kinds of one-time password tokens do not directly themselves defend against man-in-the-middle attacks, there are other technical measures that can be employed. While we get a bit twitchy about saying too much about that in public, because we do not want to tip the bad guys off as to the kinds of ways that we can detect it, none the less they are fairly readily detectable, because of things like association with accounts to IP addresses and to machines. Essentially, a machine that has never had any activity before will suddenly see a whole spike of potential log-on attempts, and that is radically different from the pattern of behaviour that is normally associated with that user, who often will only use two or three machines themselves. So you can do a great deal on back-end fraud models. While no technological solution is perfect, I think that man-in-the-middle has been overstated as a reason not to be attempting these kinds of things.

Q634 ***Earl of Erroll:*** Do you think that we should be looking at authenticating higher-value transactions over a mobile telephone link back, or something like that?
Mr Barrett: It is certainly one option and it is one that we have been discussing within PayPal. The difficulty is that it works very effectively when it works, but it is what happens when it fails. With a consumer who attempts to perform some transaction and then cannot because their phone battery is dead, you do realistically need to provide legitimate alternatives to them. Those are precisely the situations where the criminal elements will then try to create and exploit those channels; so what you are doing is potentially just moving the fraud around.

Q635 ***Lord Mitchell:*** In 2004 *Which?* claimed that there were 200 fraudulent auctions a day on eBay. I guess two years ago is almost Stone Age territory, is it not? The British Museum complained about items stolen from archaeological digs and the Federation Against Software Theft were concerned about pirated CDs and DVDs. An awful lot more people use your services now, and I wondered if things had improved.
Mr Griffith: Generally, across the board over the years, we are constantly improving our security operations. Specific to some of the areas you are talking about, we have a program called a VERO programme—

Q636 ***Lord Mitchell:*** Called . . . ?
Mr Griffith: VERO. It stands for Verified Rights Owners. We have more than 18,000 brands and rights owners who are part of that programme. We basically provide tools which facilitate their reporting items that they find on our site that violate any kind of intellectual property that they own. The tools we provide make it very simple for them to do that, but the challenge we have is that having 105 million items on the site at any one time is just volume, and the ability to have the expertise to know what each one of those is. We do provide those tools and we rely on the rights owners to get back to us. As soon as they let us know or notify us of any copyright infringement, we remove it from the site. That is a process that is working very well. We have had that for a few years. We meet with not so much FAST but FACT, Federation Against Copyright Theft. It is a group we meet with frequently and we work in partnership with them. They help us identify different kinds of filtering technologies that might help us catch things before they get on to the website, as well as us helping to improve their reporting technology, which helps us to get things down as soon as they let us know. The agreement we have with the British Museum is very similar to that. There is basically a triangular agreement between us, the British Museum and law enforcement whereby, as soon as anything is not verified to the extent that they believe is right or they do not believe it is legitimate or authentic, they let law enforcement and us know. We take it down and law enforcement go and do their bit—basically knock on doors. So it works quite effectively.

Q637 ***Chairman:*** The evidence that eBay submitted to us pointed out that the company was an online marketplace rather than an auction house and it was not a retailer. Given that eBay is a unique phenomenon, which could exist nowhere else but online, what sort of regulatory framework for the company's activities would you regard as appropriate? Do we need new regulatory systems tailor-made for online trade?
Mr McGowan: Perhaps I could answer that. The first point I would make is that eBay is a company and the sellers who trade on eBay are subject already to all manner of regulation. Just before we came here, I was trying to jot down, off the top of my head, a list of the various regulations which apply. The examples I would cite are the eCommerce Directive, the Distance Selling Directive, the Data Protection Directive, the ePrivacy Directive, the Sale of Goods Act, the Price Indications Regulations, the Trade Descriptions Act, the Unfair Commercial Practices Directive—which will come in later this year. I am not an expert on PayPal regulation, but I know they are subject to all sorts of financial regulation, such as the eMoney Directive and various bits of regulation from the FSA. The other thing to factor into this of course is that we have, as Garreth said, at any given time 100 million items live to site and 50,000 different categories. You have all manner of regulation and legislation which applies to the sale or resale of those items. So I think that I would start from the premise that there is a huge amount of regulation out there. One of the general myths there is with the Internet is that it is a bit of a Wild-West, unregulated sphere. The reality is that, in general—and there are some exceptions to this—if it is illegal offline, it is also illegal online.

Q638 ***Chairman:*** There are cases where an auction on eBay seems to be visible to other people, and the people who do not win something get an email from somebody else saying, "You bid this and didn't win. However, I have another one". As far as I can see, that is completely fraudulent. Have you been able to stop that activity?
Mr McGowan: I might ask Garreth to say a word or two about that, but this is an area where we have been, with our safeguarding members' ID—an initiative which we have just recently launched—taking steps to anonymised the bidding IDs which are there for high-value items.
Mr Griffith: First of all, we have a legitimate functionality on the site which we call "second chance offer", which is used vastly by goods sellers on the site as a way to cross-sell and up-sell merchandise to bidders who did not win the auction but who might want to pay a little bit less for something. The vast majority of the use of that functionality is perfectly legitimate. It is actually the crossover between the spoof and the phishing that we have talked about already and this functionality, where the fraudsters, if you will, are sending out these emails—often just on a chance that you might be interested—saying, "I have this laptop. I realise you didn't win it. I'll give it to you for £100 if you pay with Western Union". Actually, it is not happening on the website; it is completely separate. It is basically an email that looks just like one of ours; you just copy the HTML and you send it through. Most of our buyers are not aware of the functionality, so they think, "That's good marketing. We'll take you up on that". This is where all of what we said before, our anti-spoof tools and technologies that we have, kick in; when we say, "Check your 'My Messages', for example, and if you get a legitimate second-chance offer it is in your 'My Messages'. Forward the email to spoof@eBay.com if you want to double-check. You will get something back telling you whether it was legitimate or not". So all those same tools apply. Also we have banned, for example, Western Union or instant money transfer mechanisms on eBay as payment mechanisms. We have worked with Scotland Yard to help us enforce that. Our messaging all the time is "Do not use these mechanisms". We have it right before you bid, and when you are about to pay. There is clear messaging in emails and on the site saying, "Do not use these mechanisms".

Q639 ***Lord Harris of Haringey:*** Are you going to say that "eBay never will email you directly" or that no one you sanction will ever email you directly?
Mr Griffith: We would not say, "We don't email you directly" because we do. We do send transaction emails saying, "You have bid on something" or "You have won something". What we do is, at the same time we email it into your in-box we email it into your "My Messages" area on eBay. What we always say is, "If you have any doubt, either forward it to spoof@eBay.com or double-check in 'My Messages'". The other thing we do is that we greet you by your name. We greet you by your user name and match it to your email address. Fraudsters cannot do that, because they do not have both. They either have one or the other or just your email. Again, that is one more cog in the multiple, easy checks that you can do to recognise the legitimate email.

Q640 ***Chairman:*** What has eBay done for the customers who have been scammed that way?
Mr Griffith: One of the things we recommend in terms in payment is, when they pay with something like Western Union, it is incredibly difficult for us because, first, it has happened off our website—it has actually had nothing to do with us: it is just an email

that was made to look like ours. Secondly, they have paid with Western Union. What we do then is try to work with the police. We ask them to work with the police and then work with us, to see if we can track down fraudsters through that mechanism. What we push quite strongly on the site is the use of PayPal as a payment mechanism. The reason for that is that there is a buyer protection programme, which covers you up to £500. The vast majority of our transactions are under £500. If you used PayPal to pay, therefore—there are certain criteria, like everything—you are then covered by the PayPal protection programme and you get your money back, which is the reason we push PayPal as a payment.

Q641 ***Chairman:*** Is it not possible for you to go after, to attempt to prosecute, the people who have imitated your website?
Mr Griffith: The example I gave you about being on the ground in Romania with the United States' secret service and the Romanian police, walking into Internet cafés and arresting people—we certainly do that. As Michael referenced earlier, we generally go after them for fraud. I forget how it is worded in the new Fraud Act, but basically identity theft with the idea of committing fraud. We find that is a better way to catch them than going after IP violation.

Q642 ***Chairman:*** You expressed concern about the applicability of the Distance Selling Directive to your type of business and the complexity of selling items into other European countries. Should we not be looking to protect consumers and ensure that their online experience is the same as they are used to offline?
Mr McGowan: We absolutely support strong consumer protection legislation. We are a marketplace of buyers and sellers and, probably more than any other Internet company, our business depends on trust. If there is strong consumer protection in place then trust is enhanced. We would therefore support that. What we would welcome, however, is greater harmonisation in consumer protection legislation. The problem we have encountered with the Distance Selling Directive is that it was implemented through a minimum harmonisation process. So you see that different Member States have implemented it differently. As a result, for example, there is a right of withdrawal in the UK for consumers which is seven working days; however, in Germany it is 14. There are also differing rules determining who bears the cost of return, depending upon the Member States. So we absolutely want to see strong consumer protection but, equally, from the sellers' standpoint we want to make sure that they are not faced with a patchwork of different legislation which then becomes hard for them to enforce. I think that it is worth making the point here that we have a very large number of small businesses who are trading on the site. We calculate it as something like 68,000 people who are dependent upon eBay sales for some or all of their income. You have a very large number of SMEs who are trading on the site, and many of them are sole traders and therefore do not have the resources to keep track of all the different types of consumer protection legislation which are there. In answer to your question, however, we very much do support strong consumer protection legislation.
Chairman: Thank you very much. We have asked you a lot of questions and you have answered them patiently and in detail. We very much appreciate your coming to talk to us. If anything occurs to you subsequently, please write to us.

WEDNESDAY 28 FEBRUARY 2007

Present	Broers, L (Chairman)	Mitchell, L
	Errol, E	O'Neill of Clackmannan, L
	Harris of Haringey, L	Patel, L
	Hilton of Eggardon, B	Sutherland of Houndwood, L
	Howie of Troon, L	

Memorandum by the Foundation for Information Policy Research

The Foundation for Information Policy Research (FIPR) is an independent body that studies the interaction between information technology and society. Its goal is to identify technical developments with significant social impact, commission and undertake research into public policy alternatives, and promote public understanding and dialogue between technologists and policy-makers in the UK and Europe.

Background

The hard information security problems nowadays mostly span technology and policy. Security failures are often due to misplaced incentives; when the people guarding a system are not the people who suffer when it fails, then one may expect less than the socially optimum level of diligence. There are many relevant examples.

1. Mass-market software vendors have so far managed to disclaim almost all liability for security vulnerabilities; thus whenever a trade-off has to be made between security and ease of use, or between security and easy programmability, security tends to be neglected. So far they have got away with telling their customers to "buy a firewall" or "buy antivirus software".
2. People whose PCs become badly infected with viruses or spyware often just buy a new PC, rather than having the old one cleaned up. This may make shops less eager to sell PCs with up-to-date software and prudent defaults; aftermarket sales of antivirus products give them a further perverse incentive. Software vendors benefit too when users upgrade or replace systems early.
3. The security of electronic payment systems depends critically on the banks who set standards and police merchants. The banking industry takes a large slice of the value of Internet business via their charges to merchants; yet UK banks are finding many ways to dump fraud risk on merchants and customers.

Globalisation matters. The Internet enables UK consumers to transact with merchants in countries with inadequate law enforcement. Such protection as they have comes through the credit card system; they can charge back goods paid for but not satisfactorily delivered. Yet the technical mechanisms—from online banking through auctions to shopping websites—evolved mainly for US markets, where consumers have significantly higher protection than in the UK. If the UK drifts too far away from US norms, then the resulting "trust gap" may create serious disadvantages for Britain's online businesses. Parliament should bring UK consumer protection up to US levels—and this means financial services as well as PCs and software.

Since FIPR was founded in 1998, we have been bringing technologists together with lawyers and economists to think about these issues. The collaboration between economists and information security experts has been particularly fruitful, leading to the birth of a new discipline of "Information Security Economics," which now has perhaps a hundred active researchers. We refer committee members to the online proceedings of the Workshop on the Economics of Information Security (WEIS), which has been held annually since 2002, and to the Economics and Security Resource Page maintained by Ross Anderson, the chair of FIPR.[1]

Collaborative work between technologists and lawyers is also important; just as economics can help analyse the theoretical allocation of risks, so law deals with their practical allocation. An early study by members of FIPR's Advisory Council showed that when introducing online banking to the UK, many financial institutions designed their terms and conditions so that the customer became liable for fraud.[2]

[1] See http://www.cl.cam.ac.uk/~rja14/econsec.html.

[2] "Electronic Commerce: Who Carries the Risk of Fraud?" N Bohm, I Brown, B Gladman, Journal of Information, Law and Technology 2000 (3).

It is timely for Parliament to consider this topic. While 10 years ago both security and policy people dealt in terms of what might go wrong with the Internet, enough people have been using it for long enough that we are starting to have good data on what actually does go wrong. Also, thanks to the last few years' research in security economics, we have some practical ideas on what policymakers could do about it.

Defining the Problem

What is the nature of the security threat to private individuals? What new threats and trends are emerging and how are they identified?

As people rely on the Internet for more, so the exposure will increase. When it was only used for personal and professional communication (say in 1990) the risk was low, being largely limited to defamation, embarrassment and perhaps plagiarism. Now that most people use it for shopping and banking, fraud is a growing problem. Once people start to rely on it for safety-critical services (eg remotely-hosted medical-records systems), failures will be able to threaten human life directly.

The last five years have seen a shift from "nuisance" threats such as computer viruses written by teenagers to show off, to fraud and other exploits designed to make money. Virus writers nowadays do not attempt to crash millions of machines, but rather to install spyware on a few hundred thousand, or to take over a few thousand for sending spam. The criminals are now specialising—rather than one-man crime operations, we see malware writers, money launderers, phishermen and so on trading with each other.

What is the scale of the problem? How are security breaches affecting the individual user detected and recorded?

Reporting and measurement are a serious problem in the UK. Many US states, starting with California, have introduced security breach disclosure laws, whereby a company suffering a security failure must notify all potentially affected data subjects. In the UK, however, a company whose systems have been compromised has every incentive to keep quiet about it, and will probably receive legal advice against notifying affected individuals. Even in egregious cases—such as when a bank discovers a "skimmer" attached to an ATM—the potentially affected customers are not directly notified. In less clear-cut cases, such as when a webserver that was carelessly designed to retain customer credit-card data might (or might not) have been hacked, there is no prospect of notification. Thus security breaches affecting the individual are typically detected when the individual complains of fraud. Such complaints are often met with hostility or denial by financial institutions, or with a demand that the customer explain how the dispute might have arisen. Without breach notification, this can be an unmeetable burden of proof. As a side-effect, we have no really dependable statistics.

How well do users understand the nature of the threat?

Their understanding appears to be variable: short-term risks such as fraudulent transactions are understood better than long-term privacy risks.

Tackling the Problem

What can and should be done to provide greater computer security to private individuals? What, if any, are the potential concerns and trade-offs?

The UK Government can make one or two specific interventions; for example, it might require new PCs to be sold with a "best before" date indicating the update status of the installed software. However, the main thing Government can do is to align the incentives better. Here the most important single change would be an upgrade to banking regulation to bring the UK into line with the US "Regulation E" which governs electronic banking. This would unambiguously place the liability for fraudulent transactions back with the banks, as it has been from time immemorial: the common-law rule, codified in S24 of the Bills of Exchange Act 1882, was that a forged manuscript signature on a cheque was null and void—a rule that could not be altered by the bank's terms and conditions.

What is the level of public awareness of the threat to computer security and how effective are current initiatives in changing attitudes and raising that awareness?

We would caution the committee against endorsing the industry line that "user education" is the solution to Internet security problems. For an industry to produce insecure products, and then expect government not merely to excuse them from liability but to spend public funds advising citizens to buy anti-virus software, is breathtaking. It combines liability dumping by the platform vendors with free advertising for the antivirus firms. Instead, Parliament should enact a security breach disclosure law as in California.

What factors may prevent private individuals from following appropriate security practices?

The typical computer user can do little to identify or mitigate technical risks. He buys a computer as a consumer electronic appliance, plugs it in and uses it; attempts to turn up the "security level" of his browser will cause some web sites to not work; he has no way of telling good security software from bad; and many of the problems are completely outside the control of even technically sophisticated users. Much of the advice on offer to the nai..ve user is also dubious. For example, users are often advised to turn on encryption on their home wireless LANs; yet when this issue was polled at WEIS 2006, a majority of delegates (and a large majority of technical security experts) publicly indicated that they do not use encryption. Experts also disregard the universal advice to change passwords frequently, as this leads to weak passwords.

What role do software and hardware design play in reducing the risk posed by security breaches? How much attention is paid to security in the design of new computer-based products?

In markets with network externalities, companies generally design products with too little security at first so as to build market share by appealing to complementers. If they succeed in becoming the dominant firm in their market, they may then add excessive security in an attempt to lock in their customers more tightly. In competitive markets, especially with complex value chains, firms typically try to dump risks—for example by telling their customers to buy third-party security products such as firewalls.

Who should be responsible for ensuring effective protection from current and emerging threats?

As with risk management in general, there is a role for the state via criminal law, and a role for private action via tort litigation and insurance markets—where the State acts as rulemaker, regulator and operator of the court system. A critical difference is the speed with which online behaviour is still evolving; there are significant changes year-on-year in patterns of fraud and abuse, which create problems for Parliament with its much slower legislative cycle. Micromanagement by Government will be impractical—another reason why Parliament should focus on getting the broad incentives right.

What is the standing of UK research in this area?

About half the research in information security, and most of the work in information security economics, is done in the USA. However there is a strong research team at Cambridge, which does security engineering and helped found the discipline of information security economics; there are also research groups at Oxford (theory and protocols), Royal Holloway (mathematics of codes and ciphers), Newcastle (dependability and security usability) and the LSE (security management).

Governance and Regulation

How effective are initiatives on IT governance in reducing security threats?

Government initiatives have mostly been ineffective—the security agencies have if anything exacerbated the problem, as their institutional incentives lead them to focus on the offensive rather than the defensive side of information warfare. Private initiatives can have some effect, in that well-managed companies are generally at lower risk of information security compromise.

How far do improvements in governance and regulation depend on international co-operation?

So far the main improvements have come about from action by ISPs. Countries that were a disproportionate source of spam have in the past had their email traffic blocked. Any international agreement that prevented this (as the Nairobi convention would in the case of voice telephony) could have serious effects.

Is the regulatory framework for Internet services adequate?

It has been barely adequate up till now—although there have been many tussles over telecoms regulation, law enforcement access and so on. Unfortunately the direction of government policymaking post-9/11 appears to be drifting in the direction of more censorship and surveillance, rather than doing things that might be useful to users.

What, if any, are the barriers to developing information security systems and standards and how can they be overcome?

These are mostly economic rather than technical. The biggest single standards issue is the anticompetitive behaviour associated with the "Trusted Computing" initiative. If the liability lay unequivocally with the parties in control of system design, much more progress would be made. Some is being made; after all, banks can only dump some of their fraud risk on customers. For example, one online bank is introducing a one-day delay plus SMS notification whenever a customer appears to order a payment to a new beneficiary. But this is not rocket science; payee nomination was a feature of the UK's first electronic banking service, introduced by the Bank of Scotland in the early 1980s.

Crime Prevention

How effective is Government crime prevention policy in this area? Are enforcement agencies adequately equipped to tackle these threats?

Computer crime has always been poorly handled by the police in Britain: current targets make it a low operational priority, and the routine rotation of officers through specialist units has made it hard for local forces to build and maintain a capability. More recently, the absorption of the NHTCU into SOCA has left a gap in the coverage of level 2 computer crime (which is most of it), and the proposed mainstreaming of computer offences may dump us back to where we were before the NHTCU was set up. Mainstreaming is good in principle, as most white-collar crimes have a computer component nowadays—a technophobic detective will soon be as disadvantaged as a detective who cannot drive. However there are significant resource / priority issues, both at the sharp end of operational training and at the back end of computer forensics. Overall, we would expect better performance if the Government were to give police forces a public set of priorities, rather than trying to micromanage them using targets.

Is the legislative framework in UK criminal law adequate to meet the challenge of cyber-crime?

More or less—the issue is not so much the law as its enforcement. Even level 2 crimes are not anybody's priority at present, and no real effort at all is being made on the spam and spyware that cost users (and industry) many billions in wasted time and resources. Even a small push here might have dramatic results. We suggest making it clear that companies who use spam or spyware as a marketing tool are breaking the law, and cannot just blame the marketing agencies they employ. A single prosecution of a blue-chip company CEO could have a massively beneficial effect on the digital ecology.

How effectively does the UK participate in international actions on cyber-crime?

These are not very effective at present. The UK is weak on security disclosure and consumer rights, while the US is erratic on enforcement. About half of all child porn websites seem to be hosted in the USA; most spyware appears to be operated on behalf of US companies; and US plans to interfere with credit-card payments to online gaming sites may unleash unregulated payment mechanisms on the world—an online re-run of Prohibition. We should try to get the best of both worlds, rather than the worst of both.

CONCLUSION

UK citizens suffer significant harm as a result of Internet security failures, which are largely due to misaligned incentives. At present the harm is largely limited to online fraud, but as more and more devices become programmable and acquire the ability to communicate, the potential for harm will spread. As more safety-critical systems come to rely on the Internet, security vulnerabilities are starting to turn into hazards.

Government cannot micromanage the information security business, most of which is in any case outside the UK. What it can do, and should do, is to ensure that people and companies have the necessary incentives to take responsibility for the consequences of their actions, online as well as offline.

23 October 2006

Examination of Witnesses

Witnesses: PROFESSOR ROSS ANDERSON, Cambridge University and PROFESSOR MARK HANDLEY, University College London, examined.

Q643 ***Chairman:*** Professor Anderson and Professor Handley, thank you very much for coming to speak to us; we appreciate you time and your willingness to come and join us. You realise where we are in this inquiry, I think. Certainly Professor Anderson spoke to us at our seminar as well. We have had many sessions already taking evidence so it will be very useful for us today to close down on some of the issues. I do not think we have a lot of members of the public with us, but I am sure they realise that there is a document outside telling people about this inquiry. Would you like to introduce yourselves and then, if you wish, make an opening statement or we can go straight into the questions. Professor Anderson, perhaps you would like to start.
Professor Anderson: I am Professor of Security Engineering at Cambridge University. My background is mathematics and hardware engineering. Over the past half a dozen years I have been involved in developing security economics as a discipline, because we have come to realise that most of the things that go wrong, go wrong from misplaced incentives at least as much as from technical errors. For my sins I chair the Foundation for Information Policy Research which is an Internet policy think tank. As for substantive matters for the Committee I set these out in the paper that you received in October last year.
Professor Handley: I am Mark Handley. I am Professor of Network Systems at UCL. Primarily I am a networking research person; I have been involved in designing network protocols and network systems for many years. I have done a lot of work in the IATF which is the main Internet standards organisation for designing Internet protocols and that sort of thing and I am the main author on quite a number of the RFC documents as to how the network actually functions, especially to do with multi-media, Internet telephony and that sort of thing. Increasingly over the last few years I have been working on the networking side of security with particular emphasis on combating denial of service attacks but we have also done work in other areas such as operating system security and things like breaking wireless encryption on wireless LANS and things like that.

Q644 ***Lord Broers:*** Let me start with the first question that we have. Do you think that security is getting better for individuals on the Internet or is getting worse?
Professor Anderson: I would think that overall things are actually getting worse. The reason for that is that over the past few years crime has become commercial. Instead of people who write viruses simply trying to infect ten million machines to impress their girlfriend, they are setting out to infect hundreds of thousands of machines in order to make money. As you have real commercial incentives for people to install Adware on computers, for people to steal credit card numbers, and as the criminal networks develop that allow these to be turned into money, so the amounts of trouble that is caused to people as a result of their activities on-line appears to be going up.

Q645 ***Lord Broers:*** Would you agree with that, Professor Handley?
Professor Handley: I would largely agree with that. The situation I think is getting worse because the stakes are getting higher. On the other hand, some parts of the industry are getting better. If you look, for example, at operating systems security, Windows Vista for example is a significant step up from Windows XP, so some parts of the space are improving but overall the stakes are getting higher and the Internet is changing from being a network which is primarily of PCs to being a network of PCs, mobile devices, televisions and telephones and all of this sort of stuff. It is being used for things which are of much more economic significance so the stakes for people using it are higher and the stakes for people who are trying to abuse it are higher. I think overall it is getting worse.

Q646 ***Lord Broers:*** What do you see as the main emerging threat?

Professor Handley: The biggest things that concern me are not quite so much about the security of the individuals as about the net effect of the Internet as a whole with all of these individual machines getting compromised and the damage that can be done on the infrastructure as we start to move towards a converged network for voice traffic for television as well as just data and the traditional Internet applications. That is the thing that concerns me as an emerging threat.

Professor Anderson: I would tend to see the biggest emerging threat as being not so much technological, although I believe there will be a lot more bad stuff, for example RFID credit cards acting together with NFC mobile phones are a particular living menace. I see also the problem of this conflict between the Internet way of doing business, if you like, whereby liability gets dumped as much as possible on the end user, and the conventional way of doing business whereby the conventional rules and liability apply. I can see that more and more businesses as they move on-line are going to test the limits of what they can get away with in terms of re-writing contracts, and this could lead to market failures. To give you an example, a couple of days ago I had to renew my car insurance and I am informed that the insurance will not pay out if the car gets stolen as a result of the thief getting the keys. In other words if you leave the keys in the car or the keys are stolen from my house then there is no pay-out. This appears to be an instance of the insurance industry following in the footsteps of the banks in respect of their Internet business. I can see that causing an awful lot of trouble in a whole lot of different sectors.

Q647 ***Lord Mitchell:*** A previous witness that we had gave us an amazing statistic which I still find quite difficult to believe but I am assured it is correct, which, I think, is that 14 per cent of people who use the Internet have had such a bad experience that they never use it again. I find that quite difficult to believe as a number but he certainly said that with some degree of certainty. Whatever the number may be, if indeed all of this becomes greater and the skills in the organised crime who have huge amounts of money to invest in this become more proficient can you see a situation where the whole industry could come under threat?

Professor Anderson: I can foresee that there will be some big crunches ahead for which some kind of legislative or regulatory intervention is necessary. If, for example, liability rules in the UK and the USA drift too far apart then we could end up putting our own industry or our own citizens at a significant disadvantage. I do not have a good enough crystal ball to see exactly where those crunches are going to come.

Q648 ***Lord Mitchell:*** I do not understand the differences between the two liabilities.

Professor Anderson: For example, if you bank on-line in the USA then Regulation E says that if something goes wrong it is the bank's fault. That basically goes back to a precedent in the 1970s when a lady disputed an ATM transaction with her bank and won. Comparable cases in the UK were lost by the customer and as a result we saw in around 2000 all the banks in the UK changing their terms and conditions so that if you accept a password from them for use on the Internet, then if anything goes wrong it is your fault. This is creating a divergence between how on-line banking works in America versus how it works in Britain. Unfortunately for us, the Internet is in effect an American creation; the tools we use—web servers, web browsers and so on and so forth—are largely developed in America for American markets and under American assumptions. If we go into this arena with substantially different consumer protections then we can expect that something is going to go wrong.

Professor Handley: I think that is a very valid point. I would not expect the whole industry to collapse but what I would be concerned about would be that a lot of the potentially strong uses for the Internet might be substantially weakened. Basically, anything that requires a significant amount of trust might attempt to find alternative ways of doing business. On the other hand, there are an awful lot of uses for the Internet where we do not require so much trust and so the cost/benefit trade off ends up better for that part of the industry. For example, I would not expect e-mail or regular web browsing to suffer substantially from that but I would perhaps expect on-line commerce to suffer and then this convergence process which is happening right now would suffer significantly.

Q649 ***Lord O'Neill of Clackmannan:*** Professor Anderson, I think we have exchanged questions and answers over similar places but further down the corridor in the Commons. You caste yourself in those days very much in the role of the Cassandra. How much have you been vindicated in your pessimism over the years?

Professor Anderson: As I recall last time we were speaking that was export controls.

Q650 ***Lord O'Neill of Clackmannan:*** It might have been that or it might have been just e-commerce in the general sense.

Professor Anderson: On the export control front that is still a live issue although I suspect it is not really the business of this Committee. This was something on which academics were talking only this week to the DTI. There are many unresolved issues about how we reconcile academic freedoms with the control that the

Government wishes to exercise at the transfer of technology to foreigners. As far as e-commerce is concerned, we have seen it flourishing in some areas but not others; we have seen it flourishing in some countries but not others. Now that we have enough data to be scientific rather than just guess about it, I am coming to the conclusion that it is things like liability which make the big difference. For example, in South Africa it is difficult to do e-commerce because the banks there take an even more defensive view than here. When we bought a ticket for my mother-in-law to visit us from Cape Town I ended up having to fax the travel agent there two pages of my passport, both sides of my credit card and so on. Speaking to colleagues in South Africa there are certainly difficulties in doing on-line business there because of the view banks take. We have to be careful that we do not end up going out on a limb and marginalising ourselves and being cut off from the benefits of globalisation.

Q651 ***Lord O'Neill of Clackmannan:*** Do you think your pessimism in those days was justified or do you think maybe you were being a little more gloomy than perhaps we needed to be? Or do you think experience has vindicated you?
Professor Anderson: I think the issue on export controls is certainly still a live one. The problems that everybody anticipated in cryptography policy—which was something else we talked about then—have not come to pass because people in practice do not use cryptography in any way that has raised the policy issues that people were concerned about then.

Q652 ***Lord Broers:*** Your evidence from the Foundation for Information Policy Research notes that as safety-critical services become reliant on the Internet human lives will be put at risk. Can you explain this in more detail?
Professor Anderson: To take an example, ten years ago we relied for primary communications on the telephone system, and it was assumed that at telephone exchanges you would have the ability to function for quite some period of time in the event of a power cut. I believe the rule was that you would have six weeks' worth of diesel sitting at the telephone exchange. That now has been cut to a few days and I hear, for example, from engineers involved in that that in order to get the electricity grid back up again after an outage the engineers have to have access to their mobile phones. On the other hand, a number of the mobile phone operators only have a few days' worth of reserved power at their switching centres and at their masts. So we have eroded quite a lot of safety margin. Another problem that we come across is that although people try to create redundancy in their networks (for example by seeing to it that backbones go two different routes along the country), the increasing number of layers of networking means that it is difficult to control your network all the way down to the physical layer, and there have been one or two cases of people suffering network outages where, unknown to them, their network provider had helpfully routed both of their channels through the same piece of fibre which then got taken out by building construction work. So yes, there are going to be problems.
Professor Handley: I believe it is more than that because what is happening at the moment is a transition from regular telephony services which Ross was primarily talking about to Internet telephony services as the primary way to provide all the phone service. BT have just started to switch off the circuit-switched telephone network; they started in Cardiff this year and it will progress over the next few years. The way BT are doing this is that they are providing it over the same network as they are providing their Internet services. They are separating them; they are doing two separate networks; they are providing a whole bunch of redundancy there; they are doing it correctly but it is the same network. Obviously they are in competition with everybody else and it is not necessarily in everybody else's financial incentive to actually provide so much redundancy and to separate things off so much. We are moving away from there being a circuit-switched telephone network at all to basically it being primarily Internet telephony, hence you get this coupling between these end systems which we see getting compromised so readily and the telephone network and increasingly the television network too as Internet television comes in. All our communication eggs are going to be in one basket and we have to make sure that that infrastructure is robust.

Q653 ***Lord Sutherland of Houndwood:*** Going back to the question of personal Internet security, in your view who should be responsible for this? Where does the responsibility lie?
Professor Handley: Responsibility really needs to lie with the people who can be effective in enabling that. That really essentially means that for the most part—not entirely, but for the most part—that cannot be the end user because most end users simply do not have the technical skills or knowledge or ability to deal with that. The question is: where should it lie? I do not think you can point to any one place, although all the places you might point at seem to try to pass the buck. Responsibility should, I believe, lie with software vendors to produce software which is at least as good as the industry knows how to produce. I do not think we can expect better than that; it will not be flawless but it should be better than it has been traditionally and you want to race to the top there, not to the bottom. Some responsibility should lie

with Internet providers. That is not to say that Internet providers should stop the end system being compromised in the first place. I do not believe it is actually possible to do that in the middle of a network. On the other hand, they probably should be responsible for some degree of monitoring of their networks and when they see an end system that is misbehaving—some of those are fairly obvious to see, not all of them—then I believe they should have the obligation to disconnect that machine from the network and follow up rapidly. Obviously another part of the story lies with the financial services industry and people who are actually providing services which are where the customer can actually be defrauded, so a fair amount of liability has to lie with the banks and the rest of the financial services industry. I do not think you can point at any one place; I think it has to be most of those and primarily not the end customer.

Q654 ***Lord Sutherland of Houndwood:*** Can you, especially in such a distributed set of responsibilities, allocate legal liability in any clear ways to follow those responsibilities? Without legal liability well, we have done our best but that is it.
Professor Handley: I think you probably can although I have to admit I am not a legal expert. If your PC, for example, gets compromised at the moment there is no real liability for the software vendors or the person who sold them the PC or anything else. The question then is: did the person who sold you that software or the person who wrote that software or whatever actually the best job industry knows how to do in writing that software? If they did then I really do not think they should be liable, but if they did not then I think some liability ought to be there. That is the part of the system where it gets compromised. Once it has been compromised then I think the liability to disconnect them, if it is possible to detect them, should lie with the ISP before that machine goes on and does lots of damage to the rest of the world. Then of course the third part of that was the financial services part and that, I think, is what Ross was talking about earlier in terms of financial liability. Again the consumer is not the person who can actually deal with this so they should not be where the buck ends of stopping it unless they have done something really stupid but for the most part that is not the case.

Q655 ***Lord Sutherland of Houndwood:*** Just to stick with the software, is it a matter of simply design or is it maintenance and upgrading of the system as new threats come to be identified and understood?
Professor Handley: I think it is a combination of the two. What we have not done a great job on is deploying defence in depth which is really the primary strategy for dealing with this. If you look at Windows Vista there are 50 million lines of code in there; it is not going to be bug free. The space shuttle has about 2.5 million parts and they blow up every 50 flights. Windows Vista is going to have failures and any operating system is the same; it is not specifically a Microsoft problem. What you can do is provide various degrees of compartmentalisation within the software so that when something goes wrong the damage is contained. We know quite a lot about how to do that. One example is an operating system called SELinux (Security Enhanced Linux) which is pretty good at doing that. Those techniques are not generally employed; they tend to get in the way of what users want to do some of the time and that is why they are not deployed. On the other hand, if liability was with the software vendors to make sure that they did the best in the industry then suddenly the incentives to overcome those usability issues are really there. I think it is possible to improve things a lot beyond where they are right now.

Q656 ***Lord Sutherland of Houndwood:*** That is a bit depressing because what it suggests is a nightmare with lawyers pursuing not wholly cashable cheques because of the distribution of responsibilities in less than completely hard ways.
Professor Handley: The goal, if you do set up any liabilities for software, has to be to try to drive the improvement of the software and not to try to punish software vendors for screwing up or even for compensating the victims. It has to try and be to improve the industry as a whole so that in the long run people are safe.
Professor Anderson: I tend to the view that the big conflict, if you like, between the old world way of doing things where you have clear liability between vendor and customer and the Internet way of doing things which is that for many years vendors have got away with disclaiming all liability—is going to have to be fixed sector by sector. It is too big and intractable a problem otherwise. I expect, for example, that if my car will crash and kill me then my widow will be able to sue Mr Volvo for an awful lot of money. I do not want that property to go away just because they have started putting software in the antilock braking system rather than making it out of analogue electronics. If we get to the point that a car needs to download a software upgrade every month—which some vendors are beginning to move towards—then what are the consequences of that? I think the way to fix that is to say to the car vendors that their liability rules will not change, they will not be able to put in a little click licence on the dashboard whereby you have to press "I accept" before you can drive the car and if they do then Parliament will override them. At present I have one of these annoying "I accept" buttons that I have to press on

the SatNav. If it goes further than that into a car as a whole then Parliament has to stop it.

Professor Handley: There is another problem which is that we traditionally regard the Internet as being composed primarily of things that resemble PCs as the end systems. That is now changing and we are having a lot of devices that are at the edge of the network which are in regular, normal customers' homes and things which are not PCs. Quite a lot of us have, for example, wireless routers. A wireless router is, in principle, a software upgradeable device but I challenge you to get most customers to upgrade those within their life time. It will not happen. Ninety-something per cent of them will never be upgraded because people do not have a clue how to do it. Microsoft have a pretty good task with Windows Update and so do most of the other operating system vendors but that is not the only device in the network. One of the big security problems that has come up just recently is people driving past people's houses and reprogramming their wireless routers because they have the default password and directing people via some third party to interrupt all of their business. We have a lot of devices out there which are not going to be solved by the mechanisms we traditionally have and that is just increasing.

Q657 ***Earl of Erroll:*** We have been told by Bruce Schneier that software manufacturers should be made liable for losses arising as a result of the frauds, but one of the other aspects of it is that you cannot make software without any bugs or flaws in it. You are going to have another consequence of that which that if you are, say, Microsoft, and you have done the operating system, you are not going to know how other people's software is going to interact with that so you are going to tend to want to lock things down to your software only. Could this be highly anti-competitive? Will it in fact stop people innovating and producing new things?

Professor Anderson: One of the things that we have learned, looking at security economics, is that companies tend to make their software insecure when they are grabbing hold of a market and then add too much security later, often of the wrong kind, in order to lock people in. Yes, I am sure that all sorts of attempts will be made to lock people in. However, in the case of Microsoft software, there would be other ways of doing it. It is true that an awful lot of the unreliability comes from applications fighting each other, but the way in which applications install themselves or are installed or uninstalled and are protected from each other is something to which Microsoft has started to pay attention, and if it were facing the correct commercial incentives it would be paying an awful lot more attention. Yes, it would be a process.

Q658 ***Earl of Erroll:*** Is the trouble not so much for Microsoft but the other person? Let us say I wrote a software programme and it was going to have to run under a Microsoft operating system, I might not be aware of some of the subtleties in the updating mechanisms or something like that, so it could inadvertently introduce a flaw into it. Who would then be liable? The safest thing, in case Microsoft feels it is partly liable, is to prevent me doing that.

Professor Anderson: Microsoft has made its fortune on having an open platform, relatively speaking, on which many, many application vendors can run their wares, so such an extreme response would not be in their commercial interest. There are going to be difficult cases where something fails because somebody installed something—package A—and software—package B—on his machine. They disagreed with each other and at a certain time the machine crashed. There are a number of ways forward. For safety-critical applications you can say this machine may not have any software on it other than the approved company configuration or whatever. Recent advances in virtualisation which Cambridge has been doing an awful lot of work on enable one to run multiple virtual machines on one PC which are separated off from each other by fairly strong software mechanisms. That is another route to take but you are going to end up eventually with some hard cases for courts to decide, where ascribing liability to this vendor or that vendor or to the user who misconfigured the machine will be a complicated question of fact.

Q659 ***Earl of Erroll:*** What is this going to do for open-source software and for freeware where someone is not even being paid for it or people are doing it for the good of the community?

Professor Anderson: What I think is going to happen with open source software is that if you buy a box, a personal video recorder from TiVo for example, and it catches fire and burns your hand, you would expect to be able to sue TiVo. TiVo use Linux software; your case is against TiVo or against Dixons or wherever you bought the TiVo from. Possibly TiVo have a case against Linux and it is then down to the open-source software community to see to it that their contracts with people who embed their software in their devices do not include unreasonable recourse or, if they do, that they have insured the risk properly. If someone like TiVo is going to use free software as a platform for its device rather than paying 20 dollars a box to Microsoft, then the obvious outcome is for them to take appropriate insurance because they know that in practice they are not going to have a very valuable recourse against the thousands of hobbyists who actually wrote Linux.

Q660 ***Earl of Erroll:*** The other thing that FIPR thought about was having a "best-before" date on the machines when they are sold because if they have been sitting in the shop for a while the software will be out of date. Do you think this is a practical thing?
Professor Anderson: I think it would be a very useful incentive for the shops to see to it that the machines are updated when they are sold. It need not be particularly onerous; it could come down to the shop supplying a DVD to the customers, these DVDs contain the relevant updates and could be distributed once a month through the shop's supply chain. That would at least see that when the device came out of the box and was initially powered up, it would not be instantly vulnerable.

Q661 ***Lord Mitchell:*** Why do they not do that?
Professor Anderson: Because they do not have to and it would cost money.

Q662 ***Earl of Erroll:*** Some of the packages now do try to connect to the Internet. The first thing they do is to check to see if there is an update, but it assumes that your Broadband connection is working which is unusual sometimes.
Professor Anderson: We would expect over time that something like this would become a standard industry best practice.

Q663 ***Baroness Hilton of Eggardon:*** It is said that the Internet was not designed to be secure. Do you think we are going to go on doing a constant sort of patching or repairing of the current system or do you think it is likely that a whole new, more secure system will be developed?
Professor Handley: I do not think we are going to have a new Internet any time soon. The network effects of having a large number of people connected to one network are really large. The idea of coming up with something different without getting there incrementally from where we are here is simply not going to happen. The only two cases I can think of where it might happen would be if the current Internet fell in a large heap for some reason and we had to rebuild it from scratch but that is a very unlikely scenario. Or if something came along which was radically better in terms of cheaper or could do things that the current Internet cannot do, but neither of those seem at all likely at the moment. I think that what we are going to have is basically a variation on the current Internet for the foreseeable future. That is not to say that we are not doing research into network architectures which are radically different, we are. Groups like mine are putting in a lot of work in that area but the intent is really not to come along and say, "Okay, here is a new Internet, please use our one", it is to try to guide where we might want to go in the future, try to see where we might want to be a long way out, and then things will have to be incrementally changed from where we are now in such a way that you do not destroy the value that is already there. I do not think we are going to have a substantially different Internet but I cannot say that I particularly blame the Internet itself for the security problems. Most of the problems we see are primarily problems with systems connected to the Internet and not with the Internet itself. Of course the two may appear to be the same thing but systems connected to the Internet change pretty quickly but the Internet design itself has not changed greatly in the last 30 years.
Professor Anderson: Perhaps a useful parallel might be to consider what is the security property that you require of the M1 motorway, given that that exists in order to take anyone who wishes to go from London to Leeds and back. You do not expect that the M1 itself will filter the traffic; you do not flag down the cars and ask to see people's passports. There are one or two security properties—we do not want terrorists to blow up the bridges—but many of the bad things that happen as a result of the M1's existence are dealt with using other mechanisms. If a burglar from Leeds comes down and burgles a house in London, then there are police mechanisms for dealing with that, and so in the medium term I expect we will have better police mechanisms for police in Leeds to collaborate with police in London if a bad man in Leeds has written a program that has affected a machine in London.

Q664 ***Baroness Hilton of Eggardon:*** There are a number of mechanisms which potentially protect the security but they are not much used. I have a whole list of acronyms here: secure BGP, secure DNS, SMTP and so on but are not much used. Is that because they do not work or because it is an area where there should be greater regulation of the security systems?
Professor Handley: They are areas where there are significant deployment costs. I believe that these areas you have just talked about which are mostly to do with the infrastructure itself are areas which desperately do need addressing and I think that the industry is moving in the right direction to address them. They have limited impact on security so far as the average Internet user is concerned; they are more to do with the integrity of the network as network. It is not quite the whole story though; some of it is how you actually look up an address in a network to go to and that would prevent some certain types of hijacking attacks. I think that these mechanisms or similar ones will eventually find their way out there because the requirement really is there, but they are probably not the largest part of the problem, at least from the point of view of the end user. From the point of view of those, there is a worry about keeping the

network itself functioning. We worry about these things but your average Internet customer probably should not worry about those things, they are not their main problem.

Professor Anderson: Back in the mid to late 1990s when we were busy designing all this stuff, we tended to take the view that Internet security was a function of the Internet not having enough features but we began to realise about six or seven years ago that this was not what was wrong with it. It was that typically one company would be guarding a system but another company or a group of people would be the people who suffered when it failed. It became clear to us that at least those security problems that were outstanding tended to be those that had both a social part and a technical part, because the stuff that could be solved easily by purely technical means has been solved.

Q665 ***Lord Harris:*** Following on this question of the architecture, I read an article quite recently—which I am afraid I do not have in front of me—which suggested that Google was investing very substantially in the architecture and capacity of the Internet. Do you think that is likely to make security better or worse, that sort of investment, that sort of ownership of capacity? Or is it irrelevant?

Professor Anderson: I think it is hard to say. There is a debate going on about this and there is a debate going on particularly in the USA about network neutrality, about whether it would be possible for your phone company to offer better service to preferred providers. I think that these issues are largely orthogonal to the main security issues.

Professor Handley: In terms of their investment in network capacity, the issues are orthogonal. There is trend which probably is good from the point of view of the end customer—although there is a balance here of course—which is that, for example, Google Mail (which is basically a web mail programme where your e-mail is dealt with on the Google server, it is stored there, they do all the antivirus checking and so forth) probably protects the end customer from those sorts of compromises much better than running that on your end system because Google have a large amount of resources to pour into that particular problem and they see an awful lot of different things go past and they can spot viruses more effectively than your average antivirus software can. The downside of course is that to get that you give up degree of privacy and you have to balance these two off against each other. From the point of view of the main concerns of most end system users the move towards network serviced based applications such as Google Mail probably is a good thing for the security of the end user but, as I said, there are privacy concerns there which you would want to bear in mind.

Professor Anderson: I would agree that if you have a web mail service like Gmail, for example, then you can expect it to be better at finding viruses simply because it is so big. If somebody does a virus run or a spam run then Google should be able to detect it almost before anybody else. There are, of course, other policy concerns about having large numbers of people running all their applications on a small number of application service providers but perhaps that is not the topic for today.

Q666 ***Lord Mitchell:*** I am interested to find out what proportion of machines on the Internet have been compromised and what are they being used for?

Professor Handley: I received this question before the meeting and I attempted to find the answer but I have failed to find the answer. I can provide a few data points from various surveys that people have done. There was a survey done a little over two years ago by AOL which showed that about 20 per cent of the machines that they surveyed had viruses and about 80 per cent had some form of spyware or adware or stuff which was benignly malicious, not as bad as a virus but not good. There was also a study done by the University of Washington about a year ago which was trying to look at web servers out there and what fraction of those actually had malicious software on them that they would serve up to the users and the answer was about four per cent which is a worryingly high fraction. They surveyed hundreds of thousands and four per cent actually had malicious software on them which would try to compromise the end users' machines. I cannot tell you what fraction of machines are compromised but I can say that the problem is obviously significant. There was a network of compromised machines which were being used as one network primarily for spamming that was discovered last year and shut down which was about 1.5 million machines under the control of one bad guy (for lack of a better word). What these compromised machines are being used for, I think by far the biggest would be spamming. Probably second on the list in terms of concerns would be things like identity theft, key logging, stealing passwords or stealing credit card information and so forth. A third major concern would be what is called distributed denial of service attack where you take a lot of compromised end systems and you flood a server with the intent of making so many requests or delivering so much traffic to it that it falls off the network. There is quite a high background rate of distributed denial of service attacks happening at this point. I would say by far the biggest is spamming.

Professor Anderson: I would say that quite possibly most Windows PCs out there on the Internet have spyware on. I have certainly found it when I have cleaned up machines at home. A much smaller proportion have actively malicious stuff, things like

botnet software; it might be a few per cent. There was an interesting and indeed shocking piece of research recently about the websites which serve up evil software. We had a paper from Ben Edelman at the Workshop on Economics and Information Security this summer where he showed a very strong adverse selection in effect here. For example, although perhaps a couple of per cent of websites might be malicious, double that number of websites having a certain TRUSTe[1] stamp of approval were malicious, and similarly, although you might have a two per cent probability of the top website you find in a Google search is malicious, you might have a four per cent probability that the top ranked ad on Google is malicious. Why? Because people who are running bad operations buy ads and buy seals of approval from careless organisations that sell them. This could have some fascinating economic effects. If everybody realised this then of course they would stop clicking on Google Ads and the thing would go bankrupt. So there are some very interesting things going on there I think.

Q667 ***Lord Mitchell:*** How much of a problem are denial of service attacks in principle?
Professor Handley: The motivation for denial of service attacks always used to be some teenager trying to knock some web server or some chat server off for kicks. The last few years they have been primarily economically motivated so there have been a large number of cases of denial of service attacks aimed at a company with the purpose of trying to extort that company into paying up to stop the attack. The gambling industry in Britain was hit fairly badly about two years ago by this until the industry as a whole realised that they should all stop paying and then they would stop being hit. Certainly most of those attacks seemed to have some financial motive, whether direct extortion or some other secondary financial motive. Those attacks are significant; they cause quite a lot of the traffic on the Internet (not as much as spam but still a significant fraction of the traffic) and a lot of effort to stop. We do not yet have any mechanisms deployed in the network to automatically stop such attacks. They are a big problem and they are very difficult for network operators to shut down effectively. The big concern, though, is that we may end up with attacks which are not just for financial reasons but for terrorism reasons or politically motivated attacks and so forth which are on a significantly larger scale.

Q668 ***Lord Mitchell:*** We do see some of these already, do we not?
Professor Handley: There was one just recently against the Internet root name servers which are a critical part of the Internet infrastructure. When they do not work, nothing else works after a certain amount of time. This was not successful but it caused a certain amount of down time for some of those servers for a while. I do not think we have yet seen a large denial of service attack aimed at what I would call critical infrastructure. Most of them have been comparatively small but the potential is certainly there. The botnet that was taken down last year of 1.5 million bots was primarily used for spamming. That is the only one that I know of that is that large. If it was aimed at pretty much any service on the Internet it would probably be able to take it down. That volume of compromised machines working together can probably take almost anything off the Internet. Anybody who has sufficient financial backing could probably get that situation so you would be very concerned in the long run that that is a serious possibility. We have not seen it yet on that kind of scale.
Professor Anderson: One of the problems is that we have not had much critical infrastructure on the Internet in the past, but this is now changing in ways that nobody is really measuring. For example, when we were worried about the millennium bug ten years ago we asked ourselves whether the Internet would go down and we concluded that if the Internet does go down for a week then so what; we would actually get some work done with no e-mails. But the world is not like that nowadays. We are seeing in the NHS, for example, that systems have been rolled out where hospitals no longer have their medical records on the premises, they have server farms at remote locations. So if you were to lose Internet services then you might find that a hospital would be reduced to operating under World War II field hospital conditions and you might not be able to get x-rays from radiology to theatre. We just do not know the extent of this.
Professor Handley: We do not really understand the interconnection of the systems that use the Internet so if they went down for a week how much of the food supply system is critically dependent on the Internet? How about the electricity in the street? We simply do not know the interconnections there. The concerns are real and these denial of service attacks whilst at the moment are probably not going to cause the structure of the nation to fall apart, you would worry about that in ten years' time.

Q669 ***Lord Mitchell:*** Many of the attacks seem to come from insecure machines. Should we be forcing ISPs to do more to fix the machines and, if so, should that be through incentives or legislation?
Professor Handley: We should absolutely be doing more to make sure that ISPs are looking for compromised machines and also shutting them down as soon as possible. I think that it is probably best done through incentives rather than legislation; legislation is a pretty blunt tool for this sort of thing.

[1] See www.truste.org.

I think we really do need to make sure that the expectation is that they are looking for these kinds of attacks, and not everybody is. It does not necessarily cause them a problem if these machines are going out and attacking somebody else but it certainly causes the victim a problem. They should shut them down fairly quickly. Their customer service costs are quite significant in doing this so they are going to bear costs from doing it and they have to take that into account so there has to be some incentive to make up for that.

Q670 ***Earl of Erroll:*** Would you just tell the ISP to disconnect someone's machine arbitrarily from the Internet or would you tell the ISP to do something about the botnet or whatever is sitting on it?
Professor Anderson: What current systems do, as I understand it, is that if someone's machine is detected to be infected and sending out spam then the ISP will wall it off and allow it only access to a website from which it can download some antivirus software. This is something that it already done and for which incentives already exist. An ISP whose customers send out too much spam risks getting cut off by other ISPs and thereby having its costs pushed up.

Q671 ***Earl of Erroll:*** Is there a danger of a knock-on effect on small businesses if they are suddenly taken off without warning?
Professor Anderson: That is undeniable.

Q672 ***Lord O'Neill of Clackmannan:*** We have heard evidence that suggests that the ISPs are best placed to block bad traffic before it reaches individuals. How practical is this?
Professor Handley: I do not believe the ISPs are best placed to defend the individuals. I believe they are well placed to detect when a machine has been compromised and is being used to launch an attack or being used for spamming, but I do not think they are very well placed to actually stop bad traffic. The problem is that any bots you put in the middle of the network watching the traffic going past has incomplete information about how the end system will work. It has very incomplete information about what that end system is trying to do if it is not run by the same organisation as that end system. So one side is that they will block legitimate traffic and the other side is that bad traffic can get passed them without being detected simply because the bots in the middle simply does not know exactly how the end system will deal with various traffic. I do not believe that it is feasible for the Internet providers to be the main source of defence for their customers. They might be able to do something but I think at best it is a small part of the story and at worst they could cause significant damage. They may also significantly harm the process of innovation in the network by trying to embed into the network the concept of today's applications whereas if you actually look at how the Internet has evolved we have never been able to foresee more than five years on what the killer application will be coming up and if you embed in the Internet providers the concept of "this stuff that looks exactly like today's good traffic is good and everything else is bad" then you harm the future and we would really prefer that not to happen.
Professor Anderson: I think that is all fair enough when it comes to filtering in-coming stuff and indeed in America network neutrality is about whether ISPs are allowed to delay certain types of traffic to their customers. ISPs who also happen to be phone companies, for example, may disrupt incoming Voice over IP traffic so that their customers cannot cut their phone bills by making their long distance calls by VoIP. However, I think that there is a role for ISPs in blocking outgoing traffic. A number of ISPs already block outgoing spam. They are well placed to do this technically because the ISP, if it is of any size, may get some proportion of the spam that its own customers' infected machines are sending out. It is possible that if distributed denial of service becomes a real problem that there might be some kind of egress filtering device that helps with that as well. Ingress filtering, I agree, has got a number of problems and is tied up with policy and commercial issues.

Q673 ***Lord O'Neill of Clackmannan:*** We have also been told of the end-to-end principle. What happens if you block the traffic in the middle of the net? Can this be seen as casting in stone the system so that future improvements could be made more difficult?
Professor Handley: Yes, absolutely. We are already seeing this to some extent. Most commercial sites and universities and so forth have some form of firewall which is a boundary at their site which filters some of the traffic. Those sites have the advantage that they at least have some clue what their systems are trying to access. There is an arrangement basically between the person who runs the firewall and the person who runs the end system and they use the same organisation so in principle they are not battling each other. If you tried to do the same thing between an Internet provider and their customers they are not the same organisation so it is much harder to tell exactly what the end customer is actually trying to do. There is a significant risk of harming innovation by embedding a concept in the core of the network in any way which is: "these are what today's applications look like". We are seeing innovation problems already with commercial sites but it would be much, much worse if you did it in the middle of the network where it is not the same organisation as the end systems.

Q674 ***Lord Patel:*** My questions concern the security breach notification laws. The view that Bruce Schneier took was that the California breach

notification laws, whilst initially effective, were not so once the media lost interest in it. The question I have for you is, do you agree with that view? Secondly, do you think we should have such laws in the United Kingdom and if so how could we make them more effective? It is also the position that the banks suggested that any loss of personal data should not be reported because it would generate more anxiety and that the companies themselves should be left to decide whether it should be reported or not. Do you agree with that?

Professor Anderson: I have some experience of dealing with banking type systems as I worked in banking 20 odd years ago and I have been an expert witness in a number of disputed cases over the last 15 years. One of the problems in the UK is that if you end up with a disputed banking transaction the onus may be put on you to explain what happened without you being given access to the information that you need to discharge that. Let me give you an example. A few months ago our local Tesco cash machine had a skimmer put on it. Had that been in California then Tesco would have been obliged to write to the 200-odd people who used the cash machine that day saying, "Dear Sir, please check your bank statements and send us the bill". Of course company lawyers do not like sending letters like that unless they have to.

Q675 ***Lord Patel:*** Why did Tesco put skimmers on?

Professor Anderson: The skimmer had been put on Tesco's cash machine by a bad man who eventually was arrested. If Tesco themselves had been putting skimmers on that would be cause for even greater concern! As it happens, the Bedfordshire Constabulary had to put an article in *Bedfordshire on Sunday* saying that anybody who used this cash machine on the Tuesday could they check their bank statements and call them. If you had not been lucky enough to read that issue of our free paper you would not have known what had happened. If you then saw thousands of pounds vanishing from your account through cash machines in London and had complained to your bank and the bank had said, "Our systems are secure, go away", then you would have been stuck. The breach notification law that is now law in more and more American States, basically fixes that problem, and there is an independent fix for it in Regulation E. I think that breach notification would be enormously effective in the UK because we start off from a much lower level of consumer rights on-line and it would mean that when bad things happen they could not be covered up with the facility that they can be covered up with at the moment. Another problem has arisen since January which is that if you go to the police and report a bank fraud they will now tell you to go and take the matter up with your bank. This is convenient to the banks and it is also convenient to the Home Office in terms of the crime statistics. However, it does actually make things hard for people who are trying to get a handle on what is going on. In one recent case it has been making it difficult for the police themselves because the police were not aware that there was one gang going round the UK putting skimmers on chip and pin terminals until some bad men were caught in Phuket in Thailand with a suitcase containing 5000 forged cards, most of them British, simply because we did not have the police reports and the dots were not being joined up. So for all sorts of reasons to do with consumer rights and policing effectiveness, security breach reporting is something that we need.

Professor Handley: I would agree completely. I think that the goal obviously is to attempt to make all of the systems that we interact with as secure as is reasonably cost effective and this seems to be a very cheap and cost effective way to make it in the bank's interests to strive to be the best. Obviously I think that Bruce Schneier's point is that it created a vast amount of bad publicity for the people who had security breaches early on and relatively minor after that. Even the relatively minor is still a significant improvement from where we are at the moment where nobody has any clue what is going on with any of these systems that we depend on all the time. It provides all the right incentives. It makes security an issue which is visible at the PR level which is necessary to actually get the financial resources within the bank applied to these kinds of problems. It also provides information for the customers to be able to choose between the different possible competing financial institutions. If there is a bank which is repeatedly issuing security alerts and the other ones are not, it is not that hard to choose to go to a different bank. Right now I have no clue whether my bank is good or bad. I have tried to pay attention to these things but I just do not know because the information is not there. I think it is entirely a good thing.

Q676 ***Lord Patel:*** What about this comment that the companies should decide themselves and not report loss of personal data?

Professor Handley: I do not see that that helps anybody other than the company itself. It certainly does not help their customers and again it does not really put the incentive on the institutions to actually take security seriously.

Professor Anderson: I think it must be borne in mind that consumers in America already start from a very much higher level of protection. If you dispute an electronic banking transaction in America the bank basically has to prove that you did it using direct evidence rather than simply assertions about the wisdom of their systems or else give you your money back. The relative improvement that you got from breach notification laws in America was less than we

would expect to get here. I know that the European Union plans to bring in a directive but it is going to be a relatively narrow one to do only with the telecom systems, and I think there is a real opportunity here for Parliament to enact a much broader based breach notification law which will cover all the various relevant sectors.

Q677 ***Lord Broers:*** Do you have any idea as to how often holes in the wall are skimmed?
Professor Anderson: It is an industrial process. There are gangs who do it with equipment which is made, we believe, in Eastern Europe. The figures are of course not made known. The biggest scandal recently has been that the gangs have moved from cash machines to chip and pin terminals and there appear to be skimmers out there that put in the cable from the chip and pin terminal to the branch server which records all the information from the card except the PIN, and the operator gets the PIN by eyeball. That is what this particular Sri Lankan gang was using against a whole number of petrol stations in the UK. If you look at APACS figures card fraud is in nine figures. They hoped it would go down with chip and pin but it has not. We are talking in total hundreds of millions of card fraud, with certainly tens of millions of debit card fraud.

Q678 ***Lord Broers:*** Banks are not obliged to report that when they learn about it. Presumably the banks always do learn about it.
Professor Anderson: It is unclear to what extent there are good reporting mechanisms. If front line bank staff are told to simply deny that phantom withdrawals are possible when customers complain, then some customers will go away and perhaps the claims will never end up being reported. This is why it is a bad deal that you can no longer report such things to the police. If you try and report to the bank you may not succeed in reporting it. The bank may report some of the fraud that gets reported to it to APACS; what APACS reports in public is another thing. We just do not know how effective any of this chain is; we have no decent figures. Of course APACS has an institutional incentive to downplay the amount of fraud because they promised us that fraud would go down when they got the banks to introduce chip and pin.

Q679 ***Lord Broers:*** Can you see any downside from that fraud being made public?
Professor Anderson: Not at all. I think the *modus operandi* are known already to the bad guys and in this case, as in many others, security breach reporting is going to incentivise the defenders. There is significant literature on this in general among security economists because people started to question about whether vulnerabilities of an operating system should be reported through CERT or wherever, so that patches can be fixed. There were a number of models that were produced of the introduction and elimination of vulnerabilities and these were tested against experimental data. As far as we are aware from the operating systems front it is a good thing to report vulnerabilities although it is prudent, of course to allow a certain window for patches to be shipped. On the basis of that model I would say there was an even stronger incentive to report bad things that go wrong in the financial system.

Q680 ***Lord Sutherland of Houndwood:*** I would like to take a little bit further this issue of not reporting to the police. If I recall correctly the recent case in Leicestershire involving one of the big petrol station chains was picked up by an alert local police station when motorists came in and said they thought it was that particular cash machine. Is the issue that the police are no longer required or allowed to take on such reports? Do you know about the case I am referring to?
Professor Anderson: I do not know about the Leicester case but I know of a significant number of other cases. One of the most recent cases was at the BP garage at Girton in Cambridge. I have a local neighbourhood watch wanting me to go round and give a talk to them. The thing is also potentially high profile in that there is some suspicion of terrorist involvement, in particular that the Tamil Tigers are targeting Tamil speakers who work in retail, getting them to put these skimmers on. There is some evidence for this which has to do with money being taken out in places like Thailand where operational supplies are bought and shipped across to Sri Lanka. In this particular case the insecurity of chip and pin terminals may be contributing materially to war.

Q681 ***Lord Sutherland of Houndwood:*** The question really was, was there a police involvement that helped detect this because if there was that is really quite important?
Professor Anderson: The police involvement that alerted everyone to this going on was a police officer in the Thai resort of Phuket who caught a chap using white plastic and turned down a bribe of seven million baht, arrested the guy and went to the hotel room and found this large suitcase of white plastic. That is basically what caused everybody to realise that there was significant organised crime going on. Until that happened, as far as I am aware, the various policemen had been dealing with local issues and just thought it was some bad man locally. In one particular case where we assisted, the banks were unwilling to admit that skimming of a chip and pin terminal was even technically possible.

Q682 ***Lord Harris:*** You have said several times that the police standard practice is to refer people to their banks, but my understanding is that practice varies very widely. Could I just clarify that you are saying that it is standard practice always to refer people to their banks or that there are plenty of instances where that happens.
Professor Anderson: I am informed by the police officers that we have dealt with on this that since January the rule has been that they are to refer people to the banks who will be the first responders to allegations of card fraud.

Q683 ***Lord Harris:*** The rule they describe, is that in a particular force or is that a rule set for the country as a whole?
Professor Anderson: I understand that it is a rule set for the country as a whole. I could not quote the exact guidance on that.

Q684 ***Lord Harris:*** If you are able to provide us with more information that would be very interesting because my understanding was that that was not what the police were saying nationally, but that does not mean that another bit of the police are not saying that.
Professor Anderson: I will write to you on that.

Q685 ***Lord Howie of Troon:*** The more evidence I hear, the more I get dismayed. I really do. This brave world does not seem to be doing all that well. What I want to ask you is that the FIPR evidence told us quite a bit about misaligned incentives. Can you tell me where are the main areas where incentives should be realigned in order to improve security, which seems to be in need of improvement?
Professor Anderson: The main ways in which incentives can be realigned I think are areas we have already covered such as the matter of the kind of contracts that the bank has with their customers where, until very recently, there was settled law which said, for example, if you sign something with a manuscript signature then there are certain protections and that a forged signature could not be held against you and the bank was not allowed to re-write its terms and conditions so it could debit your account with a forged cheque. Of course this has changed over the last few years in respect of bankers' contracts with their customers in electronic matters. That is perhaps the single most important thing as far as the bulk of harm that has been done to people through credit card fraud and other types of financial fraud is concerned. The second set of incentives that you have are those incentives for software and service providers to provide, shall we say, more secure software and less damaging services. Here it becomes more complex. It would indeed be useful if we could get software vendors to accept more liability for the consequences of what they do but it comes more complex because of externalities. To take one example, browsers can be set to have a certain language called JavaScript on or off. If you have it on you become more vulnerable in that, for example, you can go to a web page which then tells your browser to change its DNS settings somewhere else and you then go to a phishing site instead of to a bank's website. If you do turn off JavaScript in your web browser then you find that you cannot buy a ticket from EasyJet.

Q686 ***Lord Howie of Troon:*** That seems a good idea!
Professor Anderson: So you end up with, shall we say, sub-optimal ways of working being very well embedded in the world because of hundreds of thousands of little design decisions taken by third parties. It is these externalities which cause most of the stickiness which stops us improving things directly. If Bill Gates were to ship Windows from next week with JavaScript turned off by default there would be a huge outcry from people who could not book flights or could not shop or whatever, and would find a way to turn it on and more websites would have to be re-written. It is this kind of inertia that we are up against.

Q687 ***Lord Harris:*** Can I just ask, can you not book flights with EasyJet without having JavaScript turned on? Is that such an impossibility?
Professor Anderson: There is a chap who wrote a front end for the British Rail timetable which enabled you to enquire about train timetables without using JavaScript. So yes, one enthusiast could perhaps write a shell for one website which makes the problem go away, but suppose Professor Handley were to write a front end for EasyJet you would then be trusting him with your credit card number every time you bought an airplane ticket. It is complicated.

Q688 ***Earl of Erroll:*** Is the answer that we should have some scripting languages which have certain things not embedded into them. Could someone produce a browser Java version which does not allow certain functions?
Professor Anderson: That is an interesting possibility; I should probably kick that out to my students to think about. It is unclear how you would generate a sub-set of a language that was on the one hand useful in the sense of it being sufficiently compatible with what is out there, and on the other hand not expose you to the standard vulnerabilities.

Q689 ***Earl of Erroll:*** If there were sufficient financial incentives, as you suggest, perhaps someone would do it.

Professor Handley: Again one of the possibilities here is the possibility of defence in depth. You can run these things from a sandbox so that whatever Java does it has limited ability to cause damage to your own system and at least to compromise the rest of your machine. That is not a complete solution but it restricts the damage that can be done.

Q690 ***Lord Sutherland of Houndwood:*** That would mean that if the punter like myself were to have to make choices of that kind—do I want this system or that?—we would be making it fairly blind because I would not know what I was excluding myself from by choosing this one rather than that one.
Professor Handley: Exactly, and that is where the issue of liability comes in and whether the software vendor is following what would be regarded as best practice in the industry and in the case of JavaScript the answer is probably not unless you sandboxed it.

Q691 ***Lord Broers:*** It might also be possible just to enable JavaScript for a single transaction, as it were, and then disable it again.
Professor Anderson: That is one possibility. There are some features of JavaScript that some filters do turn off, for example pop-up blockers. It is a difficult problem because of the assumptions of compatibility which are built into so many websites. Ultimately, when trying to design such things, you are not designing for geeks because geeks can look after themselves. I always ask myself when such questions come up, "Well, what about my mum?"

Q692 ***Lord Howie of Troon:*** Is this an area where regulation might be appropriate?
Professor Anderson: The problem prima facie with regulations is that Britain is five per cent of the world in terms of what goes on on-line, as with GNP. There are some things where we can have leverage—things like banking regulations—and there are some things where it is difficult to have leverage such as, for example, default designs of browsers. Certainly working through the European Commission we could, over time, exert influence over fundamental architectures, and questions such as the competition policy aspects of Microsoft software end up being dealt with by DGCom rather than by the DTI for that reason. I think one has to try to figure out what the UK Parliament can usefully do and what has to go to other fora for it to be effective.

Q693 ***Lord O'Neill of Clackmannan:*** Do you think companies generally, and the banks in particular, are doing enough to prevent phishing?
Professor Handley: No, I do not think they are. I think if the banks really cared about phishing and they were losing a lot of money from it, there are definitely things they could do to combat it. I can come up with one trivial example which would be that if my bank shipped me a web browser that was their custom tailored version of the web browser and they said to me, "You will only browse from this web browser; we will not admit anything else" then a lot of the phishing problems would go away, not quite everything because phishing is a social engineering problem and you usually find some way to socially engineer people but at least it would make things an awful lot simpler for the normal user to tell the difference. That is not to say that provides a solution to the problem, but I am just trying to give you an example. There are things which the banks could do which would be inconvenient for them and the customers but would greatly solve the problem. I think they could definitely do quite a bit more. Then there are some banks which just do not seem to care. I do not have a particularly good British example but I have a Bank of America account and they are constantly sending e-mails trying to get me to try out their additional services with links to their website. That is a perfect way to get the customer to click through any Bank of America e-mail into their website which sets up their customers' phishing attacks. If they really cared about phishing they almost certainly would not be trying to get me to click through that e-mail to get to their website on a regular basis. I actually got one when I was standing outside in the security line just now.
Professor Anderson: Phishing is interesting because electronic banking was a UK invention; the Bank of Scotland in 1984 came out with the first retail system that used Prestel. That was very conservatively designed. If I wanted to pay my gas bill I would have to walk into a Bank of Scotland branch and sign a piece of paper saying, "Please pay no more than £200 a month to Scottish Gas, account number such and such". That was secure because there was no practical way for a bad guy to get money out of it. If he guessed my Prestel password he could have paid my gas bill twice and then I just would not have to pay it next month and it would not be a big deal. However, a few years ago in the dotcom rush, the banks removed these back end controls, controls of what they could do on-line and how much money you could transfer, how much you could transfer to what. The banks assumed they could make the front end authentication carry all the load. I do not think it can. The issue has not been severe for them up until last year when phishing losses went up into the £30 million to £40 million bracket. Given that most of the losses are apparently being sustained by one bank, that is into the range where it is worth the chief executive's time to spend a couple of hours thinking about the problem. If it continues growing at its current rate and goes into the hundreds of millions this year then it will get attention. I believe that what is going to have to happen is that you will restrict

people to what they can do on-line, so that if you are working from your usual PC at home then you might be allowed to pay bills up to, say, £1000 but to make large fund transfers you might have to walk into a branch and sign a piece of paper. If you are browsing from a random Internet café then perhaps all you will be allowed to do is to move money between your current account and your savings account. Let us face it, is there anybody who is going to have a legitimate need to sit down in an Internet café in Peshawar and re-mortgage his house and send all the money to an account in the Philippines? If somebody wants to do that there are four or five different government agencies who would like to interview him anyway because of the amount he has transferred.

Q694 ***Lord O'Neill of Clackmannan:*** At the end of the day can we, as individual bank clients, have confidence that e-banking is safe or are we better off signing the bits of paper and going to the bank?
Professor Anderson: I do not personally use e-banking; I walk into the branch and sign a piece of paper. For me personally the idea that I sign away my rights by accepting an electronic banking password and accepting that if anything goes wrong it is my fault, this is one bridge too far for me. I have no doubt that as phishing becomes much more prevalent and as people learn more about it, the banks will realise that there is a significant opportunity cost involved in not making secure banking available, because they have to pay people salaries to wait on me in the branch when I come in waving my cheque book. Ultimately I think we are going to go towards a more mature approach to this. A nudge in the right direction from Parliament whether by regulation or by exhortation certainly would not go amiss.
Professor Handley: I do use e–banking but I have specifically told my parents not to because I believe that I am above average in the ability to secure my machines. I do not respond to any bank e-mail no matter whether it is legitimate or not but I do not trust my parents' ability to make those same kind of decisions because they simply do not have the information to make those decisions rationally. I do not think at the moment for many people e-banking is terribly safe. It is quite notable that the different banks actually have quite different policies in terms of what they will allow you to do and what they will not allow you to do on-line. I just move house recently and one of my banks would let me move my address on-line, the other bank would not. I considered it a good thing that I had to go into the branch and show my passport to be able to move my address. I was quite shocked that one of them would let me do it with no problems at all. My American bank explicitly says that I have zero liability for any fraud. They make a big deal about the fact that you do not carry any liability if anything goes wrong through Internet banking. British banks, they push it all onto me, I carry the risk.
Professor Anderson: It must also be realised that this is not just banking. Phishing is an issue for a number of on-line commerce sites. If you have an account at Amazon, for example, somebody who gets your password could log in as you, change your address and perhaps order quite expensive goods in your name. If you own stocks and shares then somebody might somehow or another phish your account with your share registrar and could move significant amounts of your investment about. It is not just retail banking; an awful lot of on-line services as well are likely to end up in the same boat.

Q695 ***Lord O'Neill of Clackmannan:*** I had the experience last week of having a telephone conversation with my bank and being asked a number of security questions, to which all the answers could have been provided had the person even considered that I might be in *Who's Who*. When I pointed that out to them they said, "You do not have to worry because there are a lot of other things that we do that you and I would not understand". That is probably correct but it was little consolation.
Professor Anderson: It is little consolation if you end up in court against your bank and you try to rely on the things that you do you not understand. I think the judge would give you rather short shift.

Q696 ***Lord O'Neill of Clackmannan:*** Professor Anderson, your institution suggested that the UK should adopt the US Regulation E to force banks to take responsibility for electronic transactions. If the problems are caused by insecure end-user systems, is this fair on the bank?
Professor Anderson: The bank must simply take a view on what sort of end systems are out there and how users can be reasonably expected to behave, especially after they have been trained by a lot of e-mails from their bank to click on attachments, especially when banks send out e-mails that even experts cannot distinguish from spam. There was one famous case where even the bank itself thought was a phish rather than a spam. The banks must take a view on the risks and they must decide whether home banking customers will be allowed to transfer all their money or 500 dollars a day or just move it between their own accounts or do nothing at all. That then becomes a risk management decision that the bank can take and it is in a position to take it because it has an awful lot of knowledge from the industry, about what the fraud history is, it has access to an awful lot of consultancies and other people with greater expertise, and it is in a position to design systems. It can decide, if it wishes, to send all their customers a hand-held password generator in the way, for

example, that Coutts do. If this is fine for the wealthy then how come the rest of us do not also get it? Questions like this need to be asked.
Professor Handley: The bank also sees the big picture. They see what is happening across many thousands of accounts. As an end user you only see one so you have no clue what the big picture is. The bank can obviously change its policy if it sees that the trend is suddenly getting very bad. The end user is just going to get steam-rollered by that trend without knowing.

Q697 ***Lord O'Neill of Clackmannan:*** I am not really interested in the big picture; the wee picture is big enough for me.
Professor Handley: It is only the bank that has the big picture.

Q698 ***Lord O'Neill of Clackmannan:*** Your institution talked about a trust-gap with the US so that we are using US websites without US style protection. Is there a case for looking for harmonisation? We know that in accounting standards the reverse might be the argument and maybe we have embraced too much. How do you feel about this issue? We give a great deal of attention understandably to Europe but in fact so much of our financial activities are related to the US. How do you feel about that?
Professor Anderson: Indeed there are not just financial activities, there is a much broader range of issues related to competition such as the cost of goods, such as the benefits you get. Why is it that as a UK customer of an airline you only get Air Miles if you fly business class whereas as an American you get them if you fly economy? There are a hundred and one issues like this. Why is it that Britain is Treasure Island to the world's retailers? We end up paying the highest prices just about in the developed world and get the worst terms of service. That is a big, big question with a lot of facets to it. Part of the solution to it was supposed to be joining the European Union to create a bigger market in which there would be more competition, but it certainly has not been the whole of the solution. I think that a political party which decided to take a strongly consumerist view might actually find itself rather attractive at the next election. A parliament that took the view that wherever British people were paying significantly more than American people then something was wrong and something would be done about it would no doubt be very popular. That of course is a question for the other place.

Q699 ***Lord O'Neill of Clackmannan:*** CDs were one of the classic examples although there has now been quite a significant change in pricing because of the focus of attention. There are now additional currency exchange issues but are you saying that at the moment if we do not focus attention on the disparities between protection in one country and another then we do not get any action and this is where it might be up to people like us and a committee like this to focus more attention on it and require the Government to answer the anomalies?
Professor Anderson: I do not think there is a magic solution for the competitiveness gap between Britain and America; we have to look at one thing at a time. If you could hit the terms of service that card holders and bank account holders generally get in the UK that is great. If you can also look, for example, at the price of software—why is it that Vista costs the same in pounds here as it costs in dollars in America?—these things all pile up. Why do we get such a bad deal on so many fronts?
Lord Broers: It is worse than that in my experience. In hardware you pay less in dollars than you pay in pounds.

Q700 ***Lord Howie of Troon:*** In the course of this investigation we have heard quite a bit about e-crime. Is there such a thing as e-crime or is it just old-fashioned crime done in a new way?
Professor Handley: I think the majority of it is old-fashioned crime done in a new way, but there are a number of things that are slightly different. One thing is the ease with which it is to perpetrate the same crime to millions of people. That makes it quantitavely different if not qualitatively different. The other thing that is noticeably different is that most of it is international (not all of it, by any means, but a lot of it is international). That was usually traditionally not the case with most traditional crime. That makes it much, much harder to reduce crime by means of arresting the people who are responsible. You end up having to defend in other ways. There are some e-crimes that are, I guess, novel. Distributed denial of service attacks are something where I do not think there is a direct real world analogue. You get may be flash crowds in stores but it is really rather different because in distributed denial of service attacks the person perpetrating the attack is anonymous; the machines doing it are compromised machines. I think most of the attacks in terms of social engineering and fraud and so forth are regular real world crimes that have made the leap over into the electronic world. The ease of perpetuating the crime and the international nature of them I think makes them noticeably different.
Professor Anderson: Last month we got the first respectable academic survey of this of which I am aware which looked at the correlation between the up take of the Internet in America and the reported crimes in the various serious categories of interest to the FBI. It is an interesting methodology because the Internet was taken up at different rates in different US states (it was quick in Alaska perhaps because

you could say there is not much else to do there). When the figures were looked at it turns out that only three of the large number of categories of crime were affected. Two were down: crimes of sexual violence and also prostitution offences were down, which the authors of the paper believe was a substitution effect from much cheaper pornography as this was reflected only in males aged 15 to 24. The one offence that was up was the category of offence known to the Americans as 'runaways', basically teenagers running away from home. That is not further disambiguated into categories of runaway, but those are the numbers that we have. The Internet makes it easier for people to run away from home.

Q701 ***Lord Howie of Troon:*** How does the Internet make it easier to run away from home?
Professor Anderson: Presumably because somebody who wants to run away from home finds it easier to make what 30 years ago were called pen friends. There will obviously be a number of these cases where the friends are in fact predators but there are no further figures on what proportion of those runaways involve some kind of danger. These are the first numbers that we have. It must be said that these numbers are only relevant to serious federal offences and do not cover the lesser things like spam and so on, but they are the first results in. In general, apart from that, I would agree with Professor Handley that we are seeing an awful lot of old crimes being re-hashed. Fraud has always happened. Social engineering has always happened. We are seeing internationalisation and it is interesting that the police are going to start mainstreaming crime, they are going to take the view that in future many crimes will have some kind of on-line dimension. General police forces as opposed to specialists are going to have to be able to deal with that.

Q702 ***Lord Howie of Troon:*** It seems to me that the police will be required to look at crime in a different way. Are the police forces really equipped to do that? Presumably you need a high level of specialisation.
Professor Anderson: There have been serious, pervasive and long term problems with computer forensics in the UK. An awful lot of police forces are going to have to do an awful of learning in order to get up to speed. This is something on which many colleagues have been working at various levels but there is still a long, long way to go I am afraid.

Q703 ***Lord Howie of Troon:*** You mentioned the international level, I suppose that would be the dark side of globalisation. How do the police here deal with foreign criminals?
Professor Anderson: The problem is not generically different from the problem that you had 40 years ago with the widespread arrival of cars and motorways. Then there was the problem of a burglar from Birmingham who could drive to Hampstead, do a couple of houses and be back in Birmingham by breakfast time. The Birmingham police did not know the crime had happened and the Hampstead police did not know that this burglar existed. It is the same thing but on a larger scale. What makes it particularly more difficult is that many of the offences are small ones—perhaps card fraud for tens of pounds or dozens of dollars—and the people who perpetrate this have been perpetrating it in Romania against a card holder in Britain, via merchants in the USA and might reckon that nobody is going to come after them. My suggestion for dealing with volume crime of this kind is that there should be randomised enforcement. What I mean by that is that the crimes are reported, the police take a view on how serious the crimes are and allocate a score to them, roll the appropriate dice and if it turns out that this particular £10 credit card fraud comes up this month then they go after that fraudster with the same vigour with which they go after a murderer. That way you ensure that someone who perpetrates millions of £10 frauds comes into police sights eventually. However, if you simply take the view—as I am afraid police forces tend to nowadays—that 'anything below the £x million mark if it is international is too difficult for us', then you are giving carte blanche to the bad guys to engage in volume crime for low denomination transactions.

Q704 ***Lord Harris:*** Is there a danger though that if the matter came to court, the person would be tried on the basis of a £10 fraud and the penalties would be proportionate to that rather than the millions of other frauds?
Professor Anderson: That is a matter for individual judicial systems. I know Scotland is different from England in this respect and I think some attention has to be paid to that. I assume that if the police pay serious attention to someone who has done a card fraud and they trace through the servers and other things that are involved, then if the guy is involved in anything like a big scale they would end up with DVDs of thousands and thousands of other transactions to be taken into consideration. Then of course you really can extradite someone and throw the book at them.
Professor Handley: One of the problems with internationalisation of course is that these trails typically will lead through one or more countries where the laws are not well aligned with our own and even if the laws were well aligned with our own there is always the language barrier in trying to trace something through in the timescale that needs to be done to actually get the forensic evidence needed to back it up. I think the task is going to be really difficult. Ross is probably right that you do actually

have to take on some of these lower level crimes to try to trace them back otherwise you will not catch those very large numbers of small amounts, but it is going to be really difficult and this is where I suspect that the majority of the successful action will not be in catching the people responsible but in trying to prevent it in the first place.

Q705 ***Lord Broers:*** Are the FBI ahead of this?
Professor Anderson: I tend to think not. I am not a hundred per cent certain of that. Certainly when it comes to dealing with a number of classes of offence and abuses we have seen private companies taking on a private enforcement role.

Q706 ***Lord Sutherland of Houndwood:*** The FIPR in its evidence says the following: "We would caution the committee against endorsing the industry line that 'user education' is the solution to Internet security problems". Maybe it is not the solution, but does education have a part at all?
Professor Anderson: In safety critical systems it is well known on the basis of longer experience than we have here that if you have a system that is difficult to use the last thing you should do is blame and train as it is called. What you should do instead is to fix the problem. When it comes to insecurity of common software products there is certainly an obvious incentive on the companies to say that it is up to the user to buy antivirus software and when the European Network Information Security Agency (ENISA) was set up two or three years ago there was intense lobbying from industry to the effect that ENISA should not lobby the European Commission to bring in liability rules for software vendors but rather should spend its budget on educating the citizens of Europe that they should go out and buy a lot of antivirus software. I was not very happy with this because if Ford were to sell you a car that did not have seat belts and then told the DTI to run an advertising campaign telling people to go out and buy seatbelts then you would not be very impressed, would you?

Q707 ***Lord Sutherland of Houndwood:*** I take the point that there are great risks of perverse incentives here but on the other hand even if one puts a liability or responsibility for helping the education on the company so that with each package you buy there would be a good practice sheet on the front which would be intelligible to those who are not specialist in the field, some things could be more easily avoided. It is just like telling people to put locks on their windows which did actually reduce the risk of them being burgled, if only diverting the burglar to some other poor person who had not.
Professor Anderson: There is a problem with that in that the industry has been getting rid of manuals as fast as it could for the past 25 years. When I first bought an IBM PC it came with a manual; if you buy a PC nowadays you cannot get a manual, you are expected to plug it in, turn it on and figure out how to use it. Telling industry to hand out advice sheets to customers goes completely against how the industry has gone.

Q708 ***Lord Sutherland of Houndwood:*** It does not have to be sheets though. It could be that when you plug in your machine and put in the disc and the thing begins to bubble in front of you, first up is a list of good practice hints. It is not a huge project we are talking about.
Professor Anderson: It is a usability issue. The industry nowadays expects customers to be able to use these products intuitively. That being the case it should provide safe defaults. It should see to it that even if JavaScript must be turned on then the consequences of turning it on are limited to the greatest extent possible.
Professor Handley: The primary piece of user education that we give users at the moment is, "Don't open an attachment unless you are expecting it". This is ridiculous. It is completely ridiculous that our software systems are so bad that it is actually unsafe to open an attachment. This should be fixed as a technical solution but it has to have the right incentives. It is ridiculous that opening an attachment can compromise your machine. We know how to sandbox these things. There are three layers of protection between the software that is opening the attachment and what goes on. It is not that technically hard to do but the industry has not gone there because they have not had the incentive to do so. The standard thing is to tell the user to exercise some sensible judgment about this as a substitute to actually fixing the real problem.

Q709 ***Lord Mitchell:*** I do not get it. Everybody, on an increasing basis, is absolutely aware of the danger. Anybody who uses a computer realises that if some sort of virus gets in it can cause huge problems. It would seem to me that if I were Microsoft or anybody else I would have as a selling point that it is more protective against viruses. It is very interesting that the Apple advertisements being run in the US in particular actually say that Microsoft has 117,000 viruses that can affect a machine and Apple has none. I do not know whether that is true or not but they are making a selling point out of it so I am surprised it does not happen.
Professor Handley: Microsoft have clearly got security over the last few years. Their systems have got a lot better but there is still a long way to go between where they are now and where they could be. Personally I

use a Mac and I know Ross uses a Mac and we would not consider using Windows for many reasons but that is not to say that the Mac I use I do not consider to be a desperately secure machine. It is not bad but it could be a huge amount better. The main reason why Apple computers are not vulnerable is simply that their market is smaller. They do have some parts of their design which are better but if you look at the best practice in the industry it is an order of magnitude better than where we are with the main stream operators and this is coming through systems such as DSB or SELinux or some of the open source ones where people have really tried to nail these problems. They are telling a good security story; they are selling on the basis of security now but I still do not think they are quite there. We really should not be trying to educate our users around the deficiencies of a system. It is like selling a car and saying, "Don't drive down a road with bumps because the wheels will fall off". You do not do that; you try to make a car so it is a bit more robust.

Q710 ***Earl of Erroll:*** Security researchers sometimes get into trouble with the criminal law for demonstrating security problems or face civil suits when companies get upset about their findings. Do you think you and your colleagues are adequately protected?
Professor Anderson: No, I do not think we are. As you may be aware from recent changes in the Computer Misuse Act which could be interpreted by a vigorous prosecutor as saying that anybody who has hacking tools is a bad person. I understand that the Home Office is going to try to fix this by publishing guidelines for prosecutors. I do not think that is really satisfactory because guidelines for prosecutors can be changed at the stroke of a pen, you do not even need the affirmation of both Houses of Parliament as you would expect with regulation. I think this is definitely unsatisfactory.
Professor Handley: I would agree completely for basically the same reasons. We do work which is in a grey area as regards the way the law is written, not necessarily the way it is enforced. Last year's Police and Justice Act definitely has terms in there which make security research and trying to figure out where things are vulnerable risky as an activity.

Q711 ***Earl of Erroll:*** Has this discouraged people from going into the area?
Professor Handley: I do not think there have been any prosecutions in the area so I suspect not.
Professor Anderson: It has caused some anxiety at other universities who teach security courses about whether they can let their undergraduates have access to certain tools.

Q712 ***Earl of Erroll:*** Is proactively looking for flaws a good thing? Are we better off not knowing?
Professor Anderson: This was the argument about security vulnerability disclosure in general in operating systems and I think we have kind of settled that. Disclosure is a good thing. Certainly there are abstract models and we have produced one of them which shows that in a perfect world disclosing vulnerabilities helps the attackers and the defenders equally. However, as the practical world deviates from these ideal models, disclosure is usually advantageous.

Q713 ***Earl of Erroll:*** I must say that sometimes I feel like that old principle that if you are in a group of people running away from a bear the only important thing is not be the slowest.
Professor Anderson: The problem with having legal uncertainty about what to do is that then the incentive on academics is not to be the most outspoken: do not criticise GCHQ, do not criticise the banks, do not point out that the Home Office is messing up with its reporting guidelines and so on; do not ever irritate somebody who might then be in a position to do a bad thing. That is not good.

Q714 ***Lord Harris:*** Could I ask whether you have come across any evidence of the corporate sector not wanting to find out about how secure their systems are because if they knew they would be more liable because they have identified something and perhaps not done enough about it?
Professor Anderson: There are plenty of cases like that. Just last week we had a banking delegation visit us who said they would really rather that such research was not done. We are simply explaining what the bad guys are already doing.

Q715 ***Lord Broers:*** Can I finish with a question about traceability? Professor Handley was talking about the difficulty of finding where things come from, particularly with certain countries who do not behave in a transparent way. If every country did behave in a transparent way, are the electronic switching systems that are used in networks that are built by companies like Cisco capable today of recording every act they take?
Professor Handley: No, they are not. The basic network itself is not capable of recording what goes through it at anywhere near the sort of rates that you would have to record everything that had gone on. There was a quote from one of my colleagues who was developing fast Internet switches a while back which is: "We can count them or we can switch them but we can't do both". If you actually wanted to store all of the data that was exchanged you probably can, at least at the edge ISPs, record information about the connections that go on and which machine

connects to which. It is not cheap to do but it can be done. Certainly at the level of e-mail there are now requirements to do this but for all the other traffic no, the technology simply is not there to record everything that is going on all the time, not at cost effective rates anyway.

Professor Anderson: If you look at UK universities there are about a hundred universities with Internet activity of about 2Gb per second. If the NSA wanted to wiretap everything it would take quite a few more fibres across the Atlantic to carry it across to Fort Meade and what would they do with it once it was there? The moral is that if you are going to filter traffic for any purpose—whether it is wiretapping, whether it is firewalling, whether it is censorship or whatever—you basically have to do it in real time unless you are looking at relatively small volumes of data, or a relatively concentrated focus on parts of the edge of the network.

Lord Broers: We have asked you a lot of questions and you have given us a lot of clear answers. Thank you very much. We appreciate your time and contribution. Should anything occur to you subsequently please let us have it in writing and we will include it in the evidence. Thank you very much indeed.

Supplementary letter from Ross Anderson

I owe the committee, as I recall, a few more pieces of information to supplement the testimony I gave you.

First, I was asked for further details about the arrangement under which electronic fraud is no longer to be reported to the police but to the banks, who will then report onwards to the police (perhaps via APACS) to the extent that they see fit.

I had heard of this initially from the West Mercia force, whom I was helping with an ATM fraud enquiry, and who were implementing it from January. I now understand that, according to the Met, the new reporting scheme will come into effect nationwide on 1 April.

The argument runs that at present if a citizen discovers a fraudulent entry on their bank statement, and goes to the local police station to report it, the police may refuse the report on the grounds that there is as yet no firm evidence of a loss. The citizen will be advised to talk with their bank, to confirm that a loss has occurred. Then the police will accept the report, issue the crime number, and feed it into their statistics and intelligence databases.

It is argued that this process is inefficient and tiresome, but could be streamlined by having the report made to the bank. The bank then collates the reports and passes them on to the police cheque and plastic card squad, who will investigate as seems appropriate to them.

One problem is that a fraud victim is often told by her banks that she must be mistaken, or negligent, or colluding, and in any case liable. So frauds are not investigated or even reported properly. At a deeper level, the scheme's incentives are quite wrongly aligned. The bank has every incentive to deny claims; and although banks may pay claims that are part of a clear pattern (as in the Sri Lankan case I referred to), an individual bank may easily fail to see a pattern, especially when complainants are stonewalled by the bank's branch staff. I think I referred to an incident in which a skimmer was placed on a Tesco ATM in Flitwick; if 100 cards were cloned then each issuing bank might have had complaints from a dozen customers, and it might simply never come to the bank's notice that they had all used that particular ATM. There is no incentive for the bank to be diligent in looking for such patterns.

Even if the bank issues a fraud report, the perverse incentives continue. APACS tries to present chip and PIN as a success in reducing fraud, so has an incentive to minimise fraud. Police forces, and the Home Office, similarly wish the crime statistics to go downwards.

The second point on which I promised you more information was the research paper at Softint 2007 on the effect of Internet take-up on state-level US crime statistics. The paper in question is "Pornography, Rape and the Internet", Todd D Kendall, at Fourth bi-annual Conference on the Economics of the Software and Internet Industries, 19–20 January 2007, Toulouse, France.[3] This shows that Internet uptake is negatively correlated with two categories of reported crime (rape and prostitution) and positively correlated with one ("runaways"—missing persons under 18).

The third point concerns the quality of forensic work and its relation to online risks. I have twice been consulted about the credit card frauds that took place in the context of Operation Ore. It is clear that the Landslide website at the centre of that case was a persistent target of credit card fraudsters. The evidence was however disregarded by UK investigators. In consequence, between 2002 and 2006, a significant number of raids took place on the homes of innocent citizens who had simply had their credit card numbers stolen by crooks who used the Landslide web site. A number of these citizens were wrongfully prosecuted for incitement,

[3] http://www.idei.fr/doc/conf/sic/papers_2007/kendall.pdf

in the absence of any evidence beyond the credit card statements. I understand that Duncan Campbell has sent you a copy of the judgment in the case of R v Grout. As for the worst-case outcome to date for personal Internet security, I would like to draw the committee's attention to "No evidence against man in child porn enquiry who killed himself", Ian Herbert, The Independent, 1 October 2005.[4]

The committee might care to consider what measures are appropriate to mitigate such risks to citizens in future.

13 March 2007

[4] http://news.independent.co.uk/uk/legal/article316391.ece

WEDNESDAY 14 MARCH 2007

Present	Broers, L (Chairman)	May of Oxford, L
	Erroll, E of	Mitchell, L
	Hilton of Eggardon, B	Paul, L

Memorandum by ISPA UK

ISPA UK

1. ISPA is the trade association for companies involved in the provision of Internet Services in the UK. ISPA was founded in 1995, and seeks to actively represent and promote the interests of businesses involved in all aspects of the UK Internet industry. ISPA currently has over 150 members, representing around 95% of the UK Internet access market by volume.

Introduction

2. ISPA welcomes the House of Lords Science and Technology Committee inquiry on personal Internet security, but is concerned to ensure that the nature of the Internet is not misunderstood and hopes that this response offers clarity on how ISPs in the UK are working together and with their consumers to promote personal Internet security.

3. Although this inquiry is billed as the first parliamentary study on this issue, this is an area that ISPA has been committed to addressing since its inception in 1995, as well as being an issue that has gained a significant amount of coverage recently and much interest in the political arena. The All Party Parliamentary Internet Group (APIG) visited Washington DC in February 2005 to discuss how the UK and US could lead the way in tackling various network integrity and Internet security issues, including spam, viruses, zombie computers, rogue dialers and denial of service attacks. Other government led industry groupings include the Home Office inspired Internet Crime Forum (ICF), the DTI anti-spam working group and the London Action Plan among other related initiatives.

4. ISPA's current activity on personal Internet security includes the planned annual ISPA Parliamentary Advisory Forum (PAF) to be held in January 2007 on the topic of Personal Internet Security bringing together key industry players, government officials, parliamentarians and lawyers in debate and discussion. ISPA has also recently met with the Office of Fair Trading regarding their Market Study into Internet Shopping where ISPA emphasised the ongoing work that ISPA Members are involved in to promote personal Internet security. A number of ISPA members are, for example, actively supporting the latest phase of the Get Safe Online awareness campaign.

5. ISPA is strongly committed to combating the threats to personal Internet safety. ISPA agrees with the approach advocated by UK Government emphasising shared responsibility and firmly believes that the ISP industry is only one part of the equation in response to such threats. Other parts of the equation include software companies, the formal schooling and education system including adult education, independently produced advice and guidance available online, branded product differentiation and a whole wealth of complementary approaches developed in tandem with those offering services online.

Defining the Problem

What is the nature of the security threat to private individuals? What new threats and trends are emerging and how are they identified?

What is the scale of the problem? How are security breaches affecting the individual user detected and recorded?

How well do users understand the nature of the threat?

6. ISPA members take the security of their customers very seriously and offer products and services such as consumer education material to help consumers protect themselves. ISPA strongly agrees with the Department of Trade and Industry's (DTI) approach to dealing with cyber security which advocates a three-pronged approach comprising of end user education, technical (network or provided to users) solutions and global co-operation on enforcement.

7. However, it is important not to forget that many security threats that are present online do not differ greatly from the threats that present themselves to consumers offline. This includes scams known as Nigerian money transfer fraud or 419 scams which are received by post, fax and email, identity theft which can occur both through phishing attacks or letters being taking out of a dustbin and intrusion which is not merely confined to the online world.

8. There is widespread misunderstanding regarding the nature of the threat, and ISPA members are committed to working with their customers to help address this by highlighting ways users can minimise the threat and informing their customers how they can better protect themselves.

9. The increasing number of zombie computers is a prime example of a security threat that users can avoid by using the advice given by their ISP. A zombie is a computer attached to the Internet that has been compromised by various means and is often used without the knowledge of the owner to perform malicious tasks under remote direction. Most owners of zombie computers are unaware that their system is being used in this way, but with the help of their ISP could take simple steps to easily rectify the problem. Infected zombie computers are now the major delivery method of unsolicited commercial email, also known as spam. It is estimated that they send between 50–80% of all spam worldwide.[1] This is a self-perpetuating problem and it seems that many users are unaware that their system is being used in this malicious way. ISPs provide a number of solutions and products to minimise the problem and are working to inform users of the simple steps that they can take to protect themselves. In this way ISPA believes that inroads can be made into greatly reducing these types of security threats and breaches.

Tackling the Problem

What can and should be done to provide greater computer security to private individuals?

10. ISPA supports the Government endorsed multi-stakeholder approach and believes that its members have a responsibility to provide clear information for consumers and simple products for consumers to use to address the security threats that present themselves in the online world. However, an ISP should be likened to a locksmith. While a locksmith can provide an individual with a lock they cannot oblige the individual to use the lock and bolt the door. In the same way although an ISP can promote the security tools that they provide they cannot compel a consumer to make use of them. Users also have a responsibility to take reasonable measures to protect the computer and other equipment that they are using.

What, if any, are the potential concerns and trade-offs?

11. ISPs invest heavily in the development and deployment of security solutions. Consumers and ISPs alike will both benefit from a secure network which would result from an increased take up of security solutions.

What is the level of public awareness of the threat to computer security and how effective are current initiatives in changing attitudes and raising that awareness?

12. Many UK ISPs regularly run specific campaigns to promote security information. Get Safe Online (GSOL) is a joint government and industry initiative designed to help protect consumers against Internet threats. Supported by a wide grouping of industry and government, GSOL offers advice about rectifying common online security problems. Government sponsors include the Cabinet Office, DTI, Home Office, Serious Organised Crime Agency (SOCA) and the National Infrastructure Security Co-Ordination Centre. ISPA believes that joined up Industry action by the various sectors affected by the threats to online security in the UK will be the only way to fully combat online security threats. The wide range of industry participants involved in GSOL from the Communications, Banking and Security industries demonstrate that GSOL has started to facilitate this. However, while consumer awareness has been raised there is still a long way to go in changing consumer attitudes.

What factors may prevent private individuals from following appropriate security practices?

13. The major factors preventing private individuals from following appropriate security practices problem is not a lack of awareness, or an under provision of technical solutions but rather a lack of confidence and the misconception that expert knowledge is required.

[1] June 2006 study by Ironport—http://www.ironport.com/company/ironport_pr_2006-06-28.html

What role do software and hardware design play in reducing the risk posed by security breaches? How much attention is paid to security in the design of new computer-based products?

14. The industry is aware of the potential threat to its own networks and customers so products are designed with this in mind. ISPs work closely with law enforcement specialist units to gain better knowledge of how products are misused so this can be taken into account when designing new products or new versions.

Who should be responsible for ensuring effective protection from current and emerging threats?

15. We support the UK Government's multi-stakeholder approach as defined above.

Governance and Regulation

How effective are initiatives on IT governance in reducing security threats?

16. UK Government has played a significant role in reducing security threats through the various policy and advice initiatives previously mentioned in this response.

How far do improvements in governance and regulation depend on international co-operation?

17. ISPA has high hopes for the upcoming Internet Governance Forum (IGF), an international multi-stakeholder policy forum that will discuss Security as one of its topics when it meets at the end of October 2006. This will help to consolidate the international co-operation which has already been mentioned in this response, as well as being a vital component of the multi pronged approach to dealing with cyber crime.

Is the regulatory framework for Internet services adequate?

18. ISPA firmly believes that the current market based approach is fit for purpose, and should not be changed. For the past 10 years ISPs in the UK have been at the forefront of proving that self-regulation is a viable model for the Internet industry and that it works effectively. A clear endorsement of the success of this model is the approach to self-regulation adopted in the UK's Communications Act 2003 and applied by the UK's national regulatory authority, Ofcom.

19. ISPs in the UK have spearheaded efforts to help consumers use the Internet safely whilst maintaining consumers' access to the vast array of resources that can be accessed via the Internet. As a testament to the commitment of ISPs to help and support their customers, many of the tools offered by ISPs to consumers to help them manage their own online experience have developed over time as new issues arise. A number of ISPs currently provide access to forms of parental control that users can apply themselves through a selection of various levels of protection. Equally, ISPs provide advice and guidance on how to avoid or prevent becoming a victim of scams such as rogue diallers or having their service compromised by a virus. It is common for users to be provided with information on how to check whether their equipment has been attacked and also, where to look for software that offers protection from such infection.

20. Most ISPs operate help lines and offer service within the framework of an Acceptable Use Policy. This has proved to be a clear benefit to users and provides transparency to a user on the actions their ISP will take to protect the service offered for all customers. This applies regardless of the type of service (dial-up, broadband, business or residential) taken by a customer and demonstrates a clear commitment on the part of ISPs to manage provision of service across the industry. Customers are given regular updates on risks associated with spam attacks and other malicious activity.

21. ISPA and its members have also taken a number of initiatives to help customers identify the appropriate contact points for specific types of concern. These include:

a. In 1996 the Internet Industry set up the Internet Watch Foundation (IWF) to provide a hotline for Internet users so illegal content hosted in the UK could be removed from the Internet. IWF figures show that in 1997, 18% of child abuse images were hosted in the UK. This figure is now down to significantly less than 0.2% due to the responsible approach by the Internet industry in the UK. Home Office Minister Vernon Coaker MP recently (September 2006) praised the UK's ISP Industry for their work over the last ten years in successfully tackling CAI hosted in the UK highlighting the importance of partnership.

b. The ISPA Code of Practice ensures members comply with a "Notice & Takedown" regime as outlined in the eCommerce Directive and UK regulations, while ensuring that ISPs are not liable for

illegal content of which they are unaware. It is currently estimated that there are over 15 billion websites around the world, with this figure ever increasing, which can be updated constantly. It is impossible, in practice, to monitor such a vast amount of content. If the Police, a judge or the IWF asks ISPs to take down illegal material then it is removed swiftly.

c. ISPA works closely with the Police and is involved in the work of the Internet Crime Forum (ICF) which looks at ways in which ISPs and law enforcement can tackle crime relating to Internet use such as chat rooms, newsgroups and on-line child "grooming".

22. The evidence shows that ISPs are committed to helping consumers and this industry wide focus has encouraged the ISPs to strive for best practice through self-regulation and the development of appropriate tools to deal with differing issues suggests this is very much the norm.

23. The ISP industry in the UK has proved that the Internet industry is working in harmony to promote safety online. This is evidence of co-operation and the ability to work together—proving that self regulation is possible and that it works.

24. However, the ISP industry is only one part of the equation in response to threats to personal Internet safety and a whole wealth of complementary approaches including formal schooling, adult education, independently produced advice and guidance available online, branded product differentiation and co-operation from all sectors of UK industry providing online services is needed.

25. ISPA firmly believes that the Lords Science and Technology Select Committee should not consider regulating the activities of ISPs as a panacea to the problem of personal Internet security. Rather, personal Internet security must be viewed as part of bigger picture. ISPs welcome being a part of the wider approach to promoting personal Internet security, but they are not the body with which the issue should end. ISPA believes that additional regulation would not be an appropriate way forward and, rather then stifling innovation, Government should support a market-based approach to producing security solutions for users and promote awareness among users on simple steps they can take to promote their own online security.

What, if any, are the barriers to developing information security systems and standards and how can they be overcome?

26. ISPA believes that strict and stringent regulation in this area would be a barrier to developing information security systems and standards, and that a flexible approach is needed in order to be responsive to problems as they arise. A technology neutral stance combined with a flexible self regulatory regime involving all relevant stakeholders and an industry-led standards process are needed in this area to safeguard future innovation.

Crime Prevention

How effective is Government crime prevention policy in this area? Are enforcement agencies adequately equipped to tackle these threats?

27. ISPA welcomed the work of the now disbanded National High-Tech Crime Unit (NHTCU) and worked closely with the team. ISPA has since established good contacts with the Metropolitan Police eCrime Unit and will continue to forge successful dialogues and partnerships with the relevant Law enforcement bodies.

Is the legislative framework in UK criminal law adequate to meet the challenge of cyber-crime?

28. ISPA supports the current legislative framework with key components including the Regulation of Investigatory Powers Act (RIPA) and the Computer Misuse Act (CMA) but would welcome more stringent remedies against spammers.

How effectively does the UK participate in international actions on cyber-crime?

29. ISPA regrets the dropping of eCrime from the G8 agenda. However, ISPA supports the UK's involvement in the various different international initiatives already mentioned in this response, and hopes that the IGF discussions will work to increase international participation. Additionally many ISPA members with an international presence participate globally in new technology groups which work on an International basis.

23 October 2006

Memorandum by the London Internet Exchange

LINX, the London Internet Exchange, is an association of Internet Service Providers and major networks, and is one of the largest Internet Exchange Points in the world.

We believe that Personal Internet Security is a complex topic requiring a blended policy approach. This should include, amongst other measures, a combination of:

- Short term educational measures to raise user awareness of practical steps that they can take now to protect themselves (eg the industry supported "Get Safe Online");
- Long terms educational measures to raise understanding of IT security principles and measures;
- Effective law enforcement action to address serious breaches of existing laws in the online environment, supported by adequate resourcing for both police and specialist computer forensics support;
- Improved international co-operation to ensure that criminal perpetrators targeting UK citizens from other jurisdictions are less likely to evade justice;
- Ongoing support by network providers, acting within an appropriate legal framework, for law enforcement efforts to trace users who commit criminal acts;
- Removal by hosting providers of material hosted on their computer servers that is illegal or unlawful to publish in the UK, when they gain actual knowledge of the existence and nature of the material.

Personal Internet security also requires the support of a wide variety of private initiatives and imperatives. A selection of examples includes:

- The wide range of consumer-orientated security-related advice available from ISPs and others;
- Ongoing improvement of security models and implementation in consumer software (eg the Windows operating system, web browsers etc);
- Ongoing development of additional technical protective systems for consumers (eg anti-virus/anti-spyware, firewalls, spam and content filters etc);
- Ongoing development of security-related services protecting end users directly or through the services they use (eg anti-spam and anti-phishing services from Spamhaus, MessageLabs, Microsoft and Mozilla);
- Aggressive competition between providers (whether of computer hardware, software or Internet services) that encourages product differentiation based on factors including innovative improvements to the security experience.

31 October 2006

Examination of Witnesses

Witnesses: Ms Camille de Stempel, Council Member, Internet Service Providers Association (ISPA), Mr Matthew Henton, Council Member ISPA, Mr James Blessing, Council Member ISPA, Mr John Souter, CEO, London Internet Exchange (LINX) and Mr Malcolm Hutty, Head of Public Affairs, LINX, examined.

Q716 ***Chairman:*** Welcome everybody, thank you very much to the witnesses for coming to talk to us today. I am going to have to ask you to make sure that you speak clearly, the acoustics of the room are not good—I apologise for that. Thank you very much for coming today and welcome to the members of the public who are here as well; I presume you picked up the note about this inquiry to tell you about the inquiry. If we could start by our witnesses please identifying yourselves and, if you wish, making an opening statement. You are so far away and the lighting is such that I cannot quite read everybody's name. Mr Hutty, perhaps you could start at this end, please.

Mr Hutty: Thank you. I am Malcolm Hutty and I am Head of Public Affairs at the London Internet Exchange (LINX). I am here with my colleague.

Mr Souter: I am John Souter, I am the Chief Executive of LINX and I would just like to say a couple of quick words about it. We are a membership organisation and we serve 250 or so Internet-related organisations who are variously ISPs, hosting companies, streaming media companies, search engines and so forth. We are one of the two or three largest in the world based on the most important metrics which are the number of members, the amount of traffic, reach in terms of routes and part of our mission is to serve our members in public affairs by doing exactly what we are doing today.

Mr Henton: I am Matthew Henton and I am on the Council of the Internet Service Providers' Association. ISPA is very pleased to be able to give evidence to the Committee today. As the main trade association for companies involved in the provision

of Internet services in the UK, ISPA has over 170 members and we represent about 95% of the UK Internet access market by volume. ISPA has been committed to providing a safe on-line experience for its users since inception in 1995. We welcome the House of Lords Science and Technology Committee inquiry and we organised the annual ISPA Parliamentary Advisory Forum in January this year on the subject of personal Internet security. That brought together key industry players, Government officials, parliamentarians and lawyers in debate and discussion; we were delighted that Lord Broers was able to speak at the event and that the Earl of Erroll was able to join us for the Panel discussion. ISPA is concerned to ensure that the nature of the Internet is not misunderstood and hopes that the evidence session will add to the written evidence that has already been submitted, offering clarity on how ISPs in the UK are working together and with their consumers to promote personal Internet security.
Ms de Stempel: I am Camille de Stempel and I also sit on ISPA Council. I also work for AOL UK.
Mr Blessing: My name is James Blessing, I sit on ISPA Council and I am Chief Operations Officer for Entanet International which is also a member of LINX.

Q717 ***Chairman:*** Thank you very much. What role do ISPs play in ensuring protecting the security of individuals using the Internet?
Ms de Stempel: We are taking a very proactive approach in the provision of personal Internet security. We take it very seriously and offer products and services such as consumer education, materials to help consumers protect themselves. ISPA agrees very strongly with the Department of Trade and Industry approach to dealing with cyber security which advocates a three-pronged approach comprising of end user education, technical solution—network or provided to users—as well as global co-operation and enforcement. We think that there is a widespread misunderstanding regarding the nature of the threat and ISPA members are committed to working with their consumers to help address this by highlighting the way in which users can minimise the threat and informing their customers how they can best protect themselves. We agree with the position of the UK Government which emphasises the shared responsibility and the belief that the ISP industries are only part of the equation in response to such threats. We also work closely with software companies and the education system to try to bring some education material into schools, developing tools to empower parents to protect their children and try to get a lot of complementary approaches which will be developed in tandem with our on-line offering.

Q718 ***Chairman:*** Do you maintain a record of what you have achieved in these various aims? For example, education of parents, do you think you understand the situation there? We have seen data that suggest only 20% of parents, if that, have a sophisticated understanding and that they are way behind their children.
Ms de Stempel: We work very closely with organisations such as Ofcom and the London School of Economics trying to look at research into why parents do not take the tools that are offered to them. What we are trying to do is map the understanding from the research in order to be able to then give better marketing of those products to parents. There is a gap, but we are aware of it and trying to address it, and we are trying to make it as simple as possible for parents to feel empowered. We think that parents at the moment feel disempowered, just because they are scared of the technologies, and we are trying to bridge that gap.

Q719 ***Chairman:*** In terms of that, is it really fair to place responsibility on the parents? In what circumstances, if any, should ISPs be held liable for security failures?
Ms de Stempel: We do not think it is about being liable, we think that we have certainly some responsibility in working with parents, working with the Government, working with the education system to make sure that parents better understand how to empower themselves in being parents. It is not putting all the onus on parents, but it is trying to get them to share that responsibility with all actors.

Q720 ***Chairman:*** You do not think, even if an ISP knows the source of information or data is fraudulent, or the players are up to perpetrating some crime, that the ISP is immune from responsibility if they pass that information or communicate between the criminals and the user, that the ISP has no responsibility?
Ms de Stempel: We have very strong terms of service so all our organisations offer very strong terms of service and if something is reported to us that is in breach of our terms of service we will take action against that particular consumer.

Q721 ***Chairman:*** Do terms of service include some validation of the honesty of your suppliers of information, for example?
Ms de Stempel: I wish we could validate the honesty of everyone, but we are trying to ensure that the consumers are aware of their rights and responsibilities as well as trying to verify as much information as we can to give them a good on-line experience with good content.

Q722 ***Lord Mitchell:*** I feel very unconvinced by what you are saying, to be honest. They are nice platitudes, but I want you to answer this question for me. Imagine that you or I are parents, unsophisticated in computers, that our child has a computer, say, from school, it takes it home. I would like to know what your industry is doing to make me aware of the dangers—not how you inform other people, but how do I know the dangers that exist on the Internet?
Ms de Stempel: On AOL specifically what we will do is that every time somebody creates a screen name we will make you go through a whole process where you have to choose the age of the person that is on line and we direct you towards parental controls where you have to either accept or not to put those parental controls on.

Q723 ***Lord Mitchell:*** Parental controls; that is an old problem. We are talking about blogging, we are talking about chat sites, we are talking about all the dangers of the Internet. How do I know about those, who is telling me?
Ms de Stempel: The media will tell you some and we also make sure that products are age-appropriate, so we do not direct children to the wrong areas, and that is how we are going to work with the media, with education, with the DfES, with the DTI to make sure that we raise awareness as to the great potential the Internet has, but also some of the dangers that exist.

Q724 ***Lord Paul:*** The Internet was built without any identity layers, that is without any means to know who and what are you connecting to. Can or should this omission be rectified?
Mr Blessing: The simple answer is that it would be incredibly difficult to rectify that problem because you are talking about rewriting, on a global scale, the entire Internet. The whole concept of identity belongs at the application layer and whatever thing you are using on the Internet should be the thing that tells you what it is you are talking to. The problem seems to be that a lot of applications are hiding that information, or making it nice and friendly so you do not see it any more, so people thing that looks right, that is fine, because they are not seeing the full details of what is going on because, to be honest, in a lot of cases it would scare them. It is an application-based issue and it is part of the whole education piece to make sure that people understand how to check someone's identity. You have a room full of people here and the only thing I have got to tell me who you are is a bit of paper in front of you; it is the same thing with the Internet. I have to go and do my research to find out who all of you are.

Q725 ***Lord Paul:*** The evidence from LINX highlights the "end-to-end principle" and the principle of "abstraction of network layers". Can you explain these principles, please?
Mr Hutty: Let me take that. Briefly, the end-to-end principle is the idea or the argument that complexity, such as things like identity management, belong at the edges of the network and not in the core of the network. By doing that they can be changed, upgraded and so forth entirely independently of the network; the network is not aware of what checks and other services are being done, whether that service is a simple identity check or an authorisation, or something like that, or whether it is something very sophisticated like the web or Voice over Internet Protocol or something like that. The end-to-end principle allows you to change what is provided at the edges without having to change the whole of the network by changing the core of the network. The linked principle of the abstraction of network layers works in the same way; instead of looking at it from the point of view of one network versus another, an edge versus the network core, it looks at it in terms of the layers on which the network is built up, so you start off with the physical layer, the wires themselves, and on top of that the networking that substantially transmits the information and on top of that the applications that provide you with basic services. By keeping all these things separate and by keeping all the complexity at the edges, we are able to create new services and to upgrade existing services over time, without having to rewrite everything and without needing the co-operation of every single party in it, it keeps things separate so that things can be done in the place where it is most effective to work. This, to our mind, has been the principle reason why the Internet has been so successful compared to other developments, because it allows everybody to bring along their own contributions without needing everybody else's co-operation.

Q726 ***Lord Paul:*** Are not these principles just an abnegation of responsibility for managing the content that travels across the Internet?
Mr Hutty: In order to apply these principles, these principles are essentially engineering principles, they are where particular tasks are done. For example, taking up your identity question, the task of identity management is performed by a server, for example a bank, and by your own computer. In order for that to happen, in order for that to allow people to arrange between themselves how things will be done and what services will be provided, it is therefore necessary from a policy point of view that the network itself is not held responsible for the traffic that passes over it because it is not in control of it. The only way of making the network legally responsible for the traffic

it carried would be to place the network practically in control of the traffic, because that is the only way to discharge that legal responsibility. The consequence of that would be that the innovation we see in the Internet would no longer be possible.

Q727 ***Earl of Erroll:*** Do you see any merit or usefulness, therefore, or a way forward on this issue is Kim Cameron's InfoCard initiative? Do you know of it?
Mr Hutty: I have seen that, I am not an expert in the specifics of that proposal, but broadly speaking I put that in the category of issues where because the Internet allows this form of experimentation, we can see people coming along and it is possible for people to come along with new and innovative approaches to those sorts of problems. You would not be able to have something like the InfoCard approach on a closed network that did not have the responsibility at the edges. For example, the telephone network or the postal network or something like that would not work in the same way. I am not a spokesman for InfoCard or something, but I would simply say that it is part of that glorious diversity of experimental approaches that has made the Internet so successful.

Q728 ***Baroness Hilton of Eggardon:*** Do you not accept any responsibility at all for filtering spam or for viruses? Viruses, it seems to me, should lie somewhere within your domain; I can understand you would not want to try and filter spam, but what about viruses?
Mr Blessing: We offer the ability for people to filter viruses and filter their spam, and these are services they can either opt into or opt out of. The reason they do not want that to happen is a lot of our customers are companies and they have the morbid fear of losing an email that might be an order for £20 million and if they lose that email and never get back to the customer—they are really paranoid about it. Because no spam system is absolutely perfect and you cannot guarantee every mail you filter is span, they say send me the mail and I will decide what to do with it. It is a question of ISPs developing choice and allowing you to either opt in or opt out of any particular business model.

Q729 ***Baroness Hilton of Eggardon:*** I can understand that in relation to spam, but in relation to viruses—
Mr Blessing: We block viruses. Unless people deliberately say no, please send me everything no matter what, we will actually scan for viruses. We cannot provide 100% reliability and we tell customers that actually they should put their own layer in there as well because the more layers doing things that you have available, the more likely are you to catch things, and again there is the issue of the false positive.

Q730 ***Chairman:*** When you say "we" what do you mean?
Mr Blessing: We as a company. It is an individual company thing. My customers are not the same AOL's customers, they are not the same as Brightview's customers, they are all very different, and it is up to you to come to a series of product offerings that solve their issues.

Q731 ***Baroness Hilton of Eggardon:*** But you do not tell us what you offer. You say that you have 170 members in your organisation.
Mr Blessing: Each individual organisation comes up with their own particular solution to the problem.

Q732 ***Baroness Hilton of Eggardon:*** But they do not tell the customers—or at least they do not tell me—what they offer in the way of scanning for viruses.
Ms de Stempel: AOL does.

Q733 ***Baroness Hilton of Eggardon:*** Your company does, but should not all ISPs offer these as an obligatory part of setting up a connection?
Mr Souter: May I speak to that? I am prompted to ask a question back: what would be the authoritative source that you would mandate as the thing to check against? You want a check to be done and certain things to be removed; where is the authoritative source of what is to be removed?

Q734 ***Baroness Hilton of Eggardon:*** That was not my point; my point was whether ISPs should automatically offer virus filtering services?
Mr Souter: My response was where is the authoritative source of what virus filtering means? I tend to agree from a personal point of view; anyone who does not make clear what they offer is doing a rather poor mistake, because they are probably underselling a service that they may offer you, but if you turn the question round and say how do you mandate that all ISPs should do that, the very first question that arises is what is the authoritative source of all this, what is it that you want removed?

Q735 ***Chairman:*** I would suggest that the ISP should offer in a transparent way that capability, so you should be offered—
Mr Souter: I think that is what my learned friends were saying they agreed with.

Q736 ***Earl of Erroll:*** Can I come at it from the other side, which is that I can see that people will have different definitions of spy ware because sometimes it is just to do advertising tracking or tracking your progress around the website, but I would have thought there is a fairly universal definition of what a virus is and I have not really heard an argument

publicly ever that something was not a virus which some people declared was, or can you give us some examples?
Mr Souter: If you take the most recent publication of one of the popular PC magazines you will see that they examined the efficacy of a wide range of existing software products and found that there was an appalling diversity of capability there.

Q737 ***Earl of Erroll:*** That is a different problem; you said what is the definition of a virus, and that is clear. The fact that the product you may be using is incapable of finding some of them, or because there is a new virus out there in the wild and your heuristic checking can not find it quickly enough in order to get the data through is a different problem, but to say that you want a definition of what is a virus is a little bit—
Mr Souter: I am not advocating that a definition be produced, I am simply trying to turn the question round and point out that the question is not such a simple question to answer. If we stay with the point which I think you were trying to make, which is that ISPs should make it clear what their offering is, there is absolutely 100% agreement amongst us, and anyone who does not do that is actually being rather foolish and Darwinism will take care of that because their services simply will not be purchased by people. If the underlying message is that people should be clearer about what is being done, I do not think there is any disagreement at all from an industry point of view.

Q738 ***Baroness Hilton of Eggardon:*** I thought I had made it quite clear that that is what I was suggesting and I am still not clear that your poor customer is going to know what the level of protection is that you are actually offering.
Ms de Stempel: For AOL what we do is we make it very clear in our terms of service that we will try to stop spam and filter viruses; however, we are also making our members aware that we might filter the problem email just because of the content that it has and we might not have known of a possible virus. We are trying to be as upfront as possible within the terms of service as to what we do, and we offer a filtered experience.
Mr Blessing: If it is a problem I would suggest that maybe it is time to change your ISP. That is simple advice but from our members' point of view they are out there to provide you with a service as a customer that you would want. If you say I want anti-virus, I want anti-spam on my account and they do not provide it, then they are not the ISP that you require.

Q739 ***Chairman:*** Do ISPs report what blocking they do?
Mr Blessing: Sorry, can you clarify, when you say "blocking" what exactly do you mean?

Q740 ***Chairman:*** I suppose they vary across the board, but does an ISP tell you that it has blocked something? There are two ways around this problem; if you block an email that you do not want blocked then presumably the ISP sends a message back to the sender of the email to say that that email did not get through—some do. I have had bank accounts where I have had a notification of a statement and that has been blocked by my ISP, but my bank then writes to me and says "Look, that email has been blocked." I find that quite satisfactory because I can then write and say "Please unblock it". I would far prefer to know that the safety precaution was there, so there does seem to be inconsistent behaviour. I would assume that ISPA has a set of rules of acceptable behaviour, does it, that you recommend to your members that you follow?
Mr Blessing: We have a series of best current practice guides that say how the industry in general should behave in particular circumstances as a policy document within the organisation. It is not a mandatory requirement that they follow those particular guides.

Q741 ***Chairman:*** You could have members who are behaving disgracefully and you would accept it.
Mr Henton: We have an ISPA code of practice as well which members must adhere to and the best common practice guidelines are bringing together knowledge from within our industry to tackle specific problems, which are not mandatory.

Q742 ***Earl of Erroll:*** We use Message Labs in Parliament and that sends you an email which says the following ones have been blocked so you can actually go to it on-line and see if they have accidentally blocked something you should have. It is very reassuring being able to see that and I can highly recommend it.
Mr Blessing: There are many different solutions as to how you represent that information to customers.
Earl of Erroll: You can send it under a subject line.

Q743 ***Chairman:*** We took evidence from Bruce Schneier and he told us that ISPs were "in an excellent position to mitigate some of the risk" to consumers, whether from spam, viruses or botnets. From a technical standpoint do you agree with that? Perhaps he was inferring that more could be done than was being done today.

Mr Henton: Could you repeat that?

Q744 ***Chairman:*** This is a quote from Bruce Schneier, that ISPs are "in an excellent position to mitigate some of the risk" to consumers, whether from spam, viruses or botnets.
Mr Henton: ISPs certainly are one part of the equation and ISPs can and in many cases do provide security solutions through security products as well as lots of security advice to consumers, but it is fair to say that ISPs are only one part of that equation. There are independent software vendors who may well be making available products that do those jobs better for certain individuals than ISPs are able to present, and there is a wider role of education. Specifically with regard to botnets, I speak for my own ISP Brightview, if we become aware that a customer's machine is compromised, usually from another ISP in fact—we would get notification that it is most likely to be sending out spam—then we would disconnect that user's machine from our network, we will contact that user and normally they would be entirely unaware that that situation had occurred and we will work with them to disinfect their machine and ensure that they are adequately protected against future infection.
Mr Hutty: My Lord Chairman, it is important to appreciate the diversity of requirements that ISPs' customers as a whole will have, and the fact that we are operating in an environment which is not static, it is changing all the time. Taking your example of sending a notice back to somebody who sent a message saying that it was blocked by a spam system, if the sender of that was a bank and it unfortunately had been blocked when it should not have been, then it is obviously ideal that they should get that message, that their message should be unblocked so they could do something about it. However, if the person who sent the message was a spammer then all that message back has done is it has confirmed that there is an active email account there that can be targeted with spam; therefore, sending that message back would actually tend to increase the amount of spam that you receive. The balance of convenience between those two is something that is a complex question that we would suggest is best weighed by ultimately the user rather than any organisation, whether it is a trade association or regulation or something, across the whole of the market for everyone. When you also take into account that whatever we do the bad guys, the people who send spam and write viruses and so forth, are finding ways around that and finding ways to exploit the very systems for protection that we might put in place, so as to increase the chances of them being able to exploit you, the user, then it is important that we have a very diverse and rapidly experimental response to these problems rather than something that is too cumbersome.

Q745 ***Earl of Erroll:*** Looking at the legal aspects of what we have just been discussing, are there actually any legal barriers to blocking spam or filtering viruses out or doing something like botnets in my spot?
Ms de Stempel: We do not think so, as long as it is made clear to consumers when they access a service as to what they are going to get and the type of filtering they are going to be subjected to, then there are no legal barriers for us to actually do that.

Q746 ***Earl of Erroll:*** You can detect sometimes that there is a botnet because you can see that a particular IP address coming into you is suddenly sending an awful lot of email when it does not normally do it and you are the people who could do it; would you be able to block that or do something about them or possibly even send something to remove that botnet?
Mr Henton: To be honest, the first step there will be to contact the customer because it might be a legitimate change in their usage pattern. I know that Dr Clayton has written some software that analyses anomaly patterns from email boxes. It is research that a lot of the industry are looking at and watching because it is very helpful to be able to co-operate so that you can tell another network when you have seen anomalous traffics from their network, and there are many organisations out there c-operating and informing each other when they spot your network using their network in some way.

Q747 ***Earl of Erroll:*** But if the customer does nothing about it—you try to contact the customer, they are out at work all day and you cannot get hold of them, what do you do?
Mr Henton: In our particular case as an ISP we shut their connection down temporarily.
Ms de Stempel: So would we. It is a good step to then educate that user as to how they can best protect themselves.

Q748 ***Earl of Erroll:*** Having shut down their connection and if they are not available on the telephone during working hours, how do you get to them to tell them what to do next?
Mr Henton: If you cannot get to them before they notice that their Internet connection is not working, they will usually phone in to our technical support line, assuming that there is some kind of technical problem and then we have obviously put a note on the account so that can then be dealt with by the support teams that we have 24/7.

Q749 ***Earl of Erroll:*** As you are replying on behalf of ISPA there are one or two very large organisations which have technical support lines which are very difficult to get hold of, if they exist.

Mr Souter: I was minded to comment about that a few minutes ago in response to one of the earlier questions. The question Lord Broers put was "is anything changing?" and the underlying theme to a lot of the questions that are being asked is not just "What is the status today?", but "Is it any better than it was a year ago or at some arbitrary point in the past?" LINX took the initiative a little while ago to talk to some of its larger members who were consumer broadband access providers in the UK and I have to say retrospectively, looking at that position a few years ago, it was pretty appalling. The AUPs, the Acceptable Use Policies, that even the very largest ISPs had did not give them a lot of latitude to take pre-emptive action in the kind of way that is implied by your question. Has anything changed? What has come from the industry side today—and we are falling into the trap a little bit of hearing a picture from three particular ISPs—if you try and generalise I would suspect that if you looked at this those AUPs have tightened up and so there is increased scope now for individual ISPs to take action of the kind that is behind your question if you like. Could you say that that is universal and a hundred per cent? Sadly, I suspect not, but then there is always going to be that kind of diversity in the market anyway. There will be people, for example, who will produce an offering, just as Malcolm said, that is designed to be the lowest common denominator, you just want access and you will take over the rest yourself. Again, if you think about what was implicit in some of the questions, it was almost implicit that there is a universality of the consumer end of the problem, i.e. everyone is on Windows PCs and therefore that defines, if you like, the nature of the problem. I am sure there is a growing but significant minority who simply look at that and laugh and say "We do not use Windows PC, we do not want to pay for a service that is already aimed towards protecting Windows PCs because we simply do not care about them; we are using UNIX machines, Macintoshes." There is a growing diversity of other kinds of equipment that is connected to the network and the solutions that may be available to them will be totally different from, if you like, the very broad range—and it may be more than 90% of the market—of those other systems. The other point that was interesting, going back to this question of has anything changed, I do not want to give over-reassurance but I recall a time from personal experience where, if you contacted your ISP and foolishly said that you were in a network at home, the very first thing they would say to you in response—and I am thinking about some of my friends here—was, "We do not support that". In other words you were actively discouraged to use a router and actively discouraged to be sitting your end user device behind network address translation which provides a very crude level, a first level of defence, against the kinds of things you have brought up today and you are clearly worried about. What has changed in recent times is that now the ISPs positively encourage you to have a network at home, even if you only have one device connected, because at least then they know that the thing they are connecting to is a router and not a PC that is so easily exploitable in 2007. That definitely has changed and we are seeing some of the impact of that going on in the market. Is it enough? Is it universal? Probably not, and those may be areas that could be fruitfully explored, but it is those sorts of dynamics in the market that have changed in the last few years that perhaps would be more fruitful to study.

Q750 ***Chairman:*** I would take issue with one thing you that you said. You said that there are lots of UNIX machines and Macs and that around: there are not. There are amongst the community of experts who understand what is going on and who control it all, and that is one thing that alarms me particularly; 95% of the users still have Windows PCs and so what we are trying to look at is, are the women and men in the street sufficiently protected, or is this whole system being controlled by a series of experts who have their own view of it and want the system to remain completely open so that they can go on having their capabilities. This is a difficult issue. You could go back and look at analogies of editors of newspapers and should there be some rules that control them, but your statement that there is a growing proliferation of alternatives to Windows is not true in practice; over 90% of users still use Windows PCs.

Mr Hutty: Most of the market for consumers is held by a relatively small number of large ISPs that do provide additional value added services to support the consumer. You then asked questions about "Is this universal?" or "Are there lot of others ISPs that are not doing that?" There are a large number of small ISPs that are serving, from the consumer market, a very small proportion of the market, and you correctly identified it as a very small part of the market. Indeed, Ofcom had a recent study on niche ISPs that showed something like 680 ISPs that they identified serving about 5% of the consumer market and about 30% of enterprises. The different kind of ISPs, different from the AOLs, the BTs and the Virgin Medias will sometimes be offering different services, orientated either at the techie that you were talking about or, particularly, the business that is generally much more interested in providing its own

protection for its own purposes and will have separate requirements and separate sites and will require different resources to deal with it. When you talk about universality in this, then all these different requirements become important, but if you are talking about broadly speaking for consumers as a whole, then I accept your point but you would have to be looking not at what every single ISP is doing but instead what is common amongst those that are serving the consumer market.
Mr Souter: My Lord Chairman, I did not mean to imply that there was not a problem amongst the great majority at all; I take your point entirely.

Q751 ***Earl of Erroll:*** Might an idea be that if you want to have an unfiltered feed or connection to the Internet that you have to pass a certain technical competency exam? There was only one thing that I just want a very quick answer to, which is if you do block some emails from getting through to customers, do they have any legal redress or is it just bad luck?
Mr Henton: I do not think it has been taken to a court of law.
Ms de Stempel: If we are making it clear in our terms and conditions that there are some false positives, it is bad luck, but then when we are approached we learn about the kind of mail that a certain computer will send and then readjust our technology.

Q752 ***Lord May of Oxford:*** Do you think the UK spam laws are "fit for purpose"?
Mr Blessing: In one word, no. What is missing from them, to be honest, is any form of redress that will actually make an impact. At the minute the maximum fine is around the £5,000 mark and if you are a spammer and you are pumping out millions of emails, the odd £5,000 fine is not going to actually make any difference to your operation, it is just a cost of business as far as they are concerned. I do know that AOL had some fun in the States acquiring a Porsche from a spammer and then giving it away to one of their members in compensation; that has a much higher level of impact when it comes to a spammer's operation.

Q753 ***Lord May of Oxford:*** Are there a significant number of UK-based spammers and, if so, what is being done to target them, other than to take away the odd Porsche?
Mr Blessing: When you say "spammers" are you talking about the actual corporates behind them or are you talking about the sources of spam? They are two separate issues.

Q754 ***Lord May of Oxford:*** I am talking about both.
Mr Blessing: The majority of spam is coming from botnets and most of the botnets are all over the place so spam does appear to come from all countries in a varying amount, depending on the level of piracy in a country—there seems to be some direct correlation in that the greater the degree of piracy in a country the higher the level of botnets and therefore the spam generated in a country. I know people who will refuse all emails from countries like Korea and China out of principle; they just will not even talk to those countries unless it is a recognised ISP server who has signed a contract. When it comes to the actual spammers themselves, it is very difficult to identify them.

Q755 ***Lord May of Oxford:*** There is a complication in the follow-up question I was going to ask you, I was going to say do ISPs have a right to prosecute spammers in the UK in the way that Microsoft, for example, through MSN has prosecuted spammers in the USA? If so, has any use been made of this right? I conjecture from that answer that you are going to say it is all too difficult.
Mr Blessing: At the minute the only person that appears to be able to prosecute the spammer is the individual end user who has to be not using the email address for any form of business, so it has to be your own personal email address, in which case you can have a go. If you are a business you are expected to take spam.

Q756 ***Lord May of Oxford:*** In an ideal world what would you do to improve things?
Mr Blessing: To be honest, the majority of spam or the causes of spam are outside the UK. The best thing we could do is take away Windows from end users and allow us to have the ability to sue people.
Mr Hutty: What James is alluding to is the fact that spam, and most of what you are considering, is essentially a security issue, it is caused in large part by the exploitation of vulnerabilities in consumer devices, in Windows PCs and so forth, and in other applications that run on the PC. These are not failures in the network per se, they are the exploitation of vulnerabilities in other things that are actually not what ISPs sell, they are not what ISPs provide. It may transit over what the ISP provides and some ISPs may see a business opportunity essentially for consumer marketing in helping to protect people, very often as a reseller, very often as a reseller of third party security products or, in the business market, an ISP might go into bespoke security consultancy, but it is all more than technical guts of the communications network. My technical response to the questions has been geared very much towards the actual running of the network with the ISP, but when you speak to a consumer-focused

organisation such as AOL here, you get responses that are very much geared around the consumer as a customer. That is seeing the ISP as a business role and the ISP as a network, but from the point of view that you were just addressing, my Lord, the ISP is not part of that but can contribute to the solution in partnership with other organisations. When it comes down to what can be done to fix it, better security of PCs is clearly the answer, but how you achieve that is not really for us to say because it is not really our business.

Chairman: That is one of the key issues of course and we have spent a lot of time on it. Last week we were talking to a lot of the suppliers of operating systems et cetera and having that conversation, and we do appreciate the complexities of that situation. At the moment though I am beginning to come to the view that too much responsibility is put on the end user and that there may be capabilities elsewhere that are not being exploited at all in trying to help. We heard an analogy made by one expert that we were talking to in Silicon Valley who equates this all to the supply of water and said what would happen to a water company if it supplied poisoned water to every household and required the household to provide the filters. It is perhaps not a good analogy but I throw it out, that opinion is around the place with certain people. Let us move, Lord Erroll, you have another question.

Q757 ***Earl of Erroll:*** There are a lot of attacks on Internet routing systems which redirect traffic to the wrong place so that the "bad guys" can intercept email, perform phishing attacks, man-in-the-middle attacks or disrupt normal service. There are systems such as "secure BGP", "secure DNS", "SMTP over TLS" and some of these might prevent such attacks but are rarely used. Why not? Is this an area for regulation or for incentives?

Mr Hutty: DNS-Sec and sBGP are experimental systems. If we were in an environment where regulation prescribed what protocols to use and that kind of level of detail, it is my belief that that regulation would not be requiring those systems because they are experimental, they are immature and they are still in process of argument about whether they actually work and whether they work bearing in mind certain flaws that have been identified or potential flaws that have been identified—I am thinking of particular things in DNS-Sec. I would suggest that these fall into the category of the Internet as being an environment that encourages the technical innovation and development of user systems and regulation should support and enable that diversity and experimentation because that delivers benefits. If we were to move to an environment where it was quite that prescriptive in regulation at a technical level, then that would very much preclude it.

Mr Blessing: The Internet depends on co-operation between users. The Internet is not a single thing, it is lots of other networks connected together, so where those networks connect there has to be co-operation and organisation between those two networks. If one side says "I am going to use this" and the other side will not support it, those two networks will not talk to one another.

Q758 ***Earl of Erroll:*** What you are really saying—which I would tend to agree with—is that regulation is not going to work because you will always be behind, but incentives might if in some way you were incentivised to move faster towards some of these more secure technologies.

Mr Hutty: The incentives are there. Take sBGP, the incentive in that is that it protects against an attack on your core infrastructure. What more incentive could you offer an ISP to protect themselves against an attack on their core infrastructure than the fact that if it is attacked and it fails then they have lost what they are providing? So the incentives are very much there.

Q759 ***Earl of Erroll:*** Earlier, in response to another question, you actually pointed out that the network is layered, you have an abstraction of network layers, and the fact that the routers can then be attacked was actually suggesting you are undermining that fundamental principle, so you should be addressing these areas using things such as SBGP or otherwise actually your abstraction network does not exist.

Mr Hutty: I hope you did not understand my answer, when I was saying it is experimental, to mean it is not something that is important or coming or going to happen; I was not being dismissive of it.

Mr Blessing: There is not the stable vendor support to operate those protocols.

Mr Hutty: But that will come.

Mr Blessing: That will come. People really want the network to be stable because it means you can provide the service. Therefore they are pushing the vendors to fix those problems; the vendors' hardware has to support the protocols otherwise you cannot implement them, and both sides have to support it. There is more than one vendor platform and until all the vendor platforms support it properly and inter-operate properly, people will not adopt it.

Q760 ***Earl of Erroll:*** Will there be a problem therefore because BT is buying its 21st CN routers from China; it is Hawaii technology. Will that be a problem?

Mr Blessing: No, because they will adopt the standards. The problem is we do not know when they are going to get them into development.

Q761 ***Earl of Erroll:*** Is this actually quite vital, because at the moment if you have got a man-in-the-middle attack, a phishing attack using a man-in-the-middle attack, one of the ways you can check as to whether there is something going on is to ring up the bank or whoever to find out whether it was genuine or not, but if you have a vishing attack at the same time, simultaneously, they could be interrupting that man-in-the-middle attack as well, so if we do not have proper security of these layers, someone could be totally vulnerable, there is no second channel over which you can all hope to get an electronic communication. Is that a problem?
Mr Blessing: You are saying—

Q762 ***Earl of Erroll:*** When you have VoIP telephony—21st century telephony is VoIP—that will be vulnerable to the same sort of attacks as man-in-the-middle attacks on the rest of the Internet, so when you try to authenticate by ringing up, that telephone call can also be hijacked I presume.
Mr Hutty: That is not necessarily true but it is possibly true depending on the implementation. As things stand it is possible to prevent those sorts of man-in-the-middle attacks. There is a balance of convenience that the banks or an eCommerce site has between allowing their customers to use their site easily and readily without going through the rigmarole of setting up and authenticating it against the security of this. The technical systems are available for them to use that will prevent a man-in-the middle attack; the technical systems are available for deployment against other applications and that would include VoIP. I am not going to speak to the 21CN thing because I do not think it is appropriate, you would need to speak directly to BT about that, but in principle the broader question is that man-in-the-middle attacks are a solvable problem; but they do entail a balance between security and ease of use at the moment.

Q763 ***Lord Paul:*** The Government wants consumer ISPs to block access to child abuse image websites. Is this practical and will it work?
Mr Henton: The Home Office has made its intention clear that by the end of 2007 it wants all ISPs offering broadband Internet connectivity to the UK public to have implemented systems for blocking access to child abuse images and child abuse websites. A good many ISPs have already implemented a form of blocking technology which does block those images that are identified by the Internet Watch Foundation and put onto their child abuse database. In that sense you could argue that it is practical because it is being done. My own company Brightview implemented this back in 2004, but I do not think content blocking in this way should be seen as a panacea. We need to make an important distinction between a deliberate concerted attempt to distribute and to access paedophile material and an accidental downloading of a piece of material. Blocking the IWF list will protect consumers who might accidentally go onto a website where such images exist; it is unlikely to stop a determined paedophile because they are always going to find a way around such blocking technologies; it is difficult to circumvent them and, in fact, there is a very strong argument that employing blocking technologies will actually drive paedophile activities underground into the so-called dark net where it is impossible to actually trace their activities. That could have consequences in terms of trying to secure prosecutions against those people.

Q764 ***Lord Paul:*** What other sorts of traffic would these systems block and how does the "end-to-end principle" interact with the blocking system?
Mr Blessing: In theory it can block anything as long as you know what you are blocking. If you can come up with an absolute list that says this must be blocked, you can block it, but unfortunately doing that completely destroys the end-to-end principle; it means that people could potentially put controversial things—we have this protest going on outside at the minute about weapons of mass destruction and, potentially, a website discussing that particular topic could end up on that block list, at which point no one could view it if that block list was enforced. It completely destroys the point. The other thing it does is it adds a layer of complexity to the network. Something that has been discussed a number of times by different people is potentially it would revoke the mere conduit status of an ISP and make them liable for blocking stuff they do not know about, which has not been decided one way or the other because no legal advice will come down on one side or the other.
Mr Henton: If I could just say, the reason why the ISP industry has generally moved towards these blocking technologies with specific regard to the IWF CIA database is the trust that ISPs have in the IWF and in the authenticity of that database and what it contains. Where the ISPs would certainly lose trust would be if other types of content were to be requested to be blocked: who would be requesting them and what would be the verification process behind what would be on any other databases.
Mr Blessing: The other particular issue with the IWF as it stands is that it is generated at points in time, it is not a live system, which means that potentially the minute it is updated it becomes out of date and anybody wishing to distribute images realises this

and they will basically change their content just after the update.

Mr Hutty: That goes directly also to Lord Paul's point about the end-to-end principle. The designers of the systems that we are referring to take a list that exists of addresses of content to be blocked; that list, as James has just said, inevitably becomes out of date all the time, although the IWF update it as fast as it can, but it also has the characteristic that it inherently ignores material that either does not have an address or material whose addresses are unknown to the IWF. The first category would include material that is simply passed around directly between paedophiles and the second would be something that is locked away in some secret area that you have to be a member to take part in, and that therefore is an inherent flaw in such a system meeting the policy objective of preventing paedophiles getting access to this material. If you were then to extend that principle so as to say the ISP ought as a gatekeeper for the Internet to be able to prevent access to all that kind of material, to be able to tell themselves what that material is, then quite apart from the essentially impossible nature of asking ISPs to make that kind of judgment, that would come down to a very low level to the technical question of infringement on the end-to-end principles to which you were referring specifically. If you ask an ISP to approve the traffic that is passing over its network and decide whether or not it is going to block it, based on its own criteria, the ISP would have to then say for each piece of material, this piece of material is okay, I will pass it on, this piece of material is not okay, I will block it. Then it will come up against another piece of material where it does not know, it does not recognise this, it cannot tell. If the ISP is held legally responsible for blocking access to illegal material, of whatever nature, then the only practical recourse for it as a business would be to block that material that it does not recognise. That practice would prevent people from deploying new protocols and developing new and innovative applications, including the security applications and systems that Lord Errol was talking about earlier, and also new services. As we put in our written evidence, just about everything you think of as the Internet nowadays—the web, modern email, instant messaging, video conferencing and voice—all those things have been implemented since the core so if you were to take that sort of policy decision that ISPs should be required to recognise what those things are and to make decisions accordingly, you will be preventing that kind of innovation and you will be turning it from what I would characterise as a communications network that connects end points that pass information to each other into an on-line service where you simply connect to the ISP and get whatever the ISP thinks is acceptable for you. That would be a major policy change and it is not a policy change that the rest of the world has been doing. One thing that I have not actually mentioned yet is that all this is in a global context as well.

Q765 ***Baroness Hilton of Eggardon:*** Are you always able to detect when your customers become part of a botnet and, if so, what do you do about it? You have told us some of the things you do in terms of communicating with them. Do you do other things like putting them in a sandbox or a walled garden and restricting access or do you just try and sort out the whole problem?

Mr Henton: We at Brightview sort out the problem on an individual user baser. We disconnect them from the network as soon as we are aware that a customer is infected and we then do not allow them to reconnect to the network until a technical support adviser is reasonably satisfied that the source of the infection has been removed and that steps are in place to prevent future infection. Only then will they be allowed to reconnect to our network. From speaking to my colleagues at other ISPs they have broadly similar policies in place.

Q766 ***Baroness Hilton of Eggardon:*** A sort of halfway house would be to restrict access rather than to use some aspects?

Mr Blessing: There are a number of ISPs who have developed sandboxes, walled gardens, bits that are limited, so they can have access to things like virus updates and can actually download new pieces of anti-virus software to clean them temporarily and also the ability to then see whether there is any anomalous traffic, whether the user is doing something when they say they are not actually using the machine and whether there is traffic passing to locations that look suspicious.

Chairman: That leads to Lord May's question, please.

Q767 ***Lord May of Oxford:*** Do you have any estimate of the number or proportion of UK machines that have a security problem, the zombies?

Mr Henton: ISPA has no such figures on the number of machines that have a security problem. However, you could argue that any computer connected to the Internet potentially has a security problem. The number of security updates from operating system manufacturers and application vendors will tell you that new vulnerabilities are being found on an almost daily basis, so the potential is there for virtually any machine to develop a security problem.

Q768 ***Lord May of Oxford:*** As I hear you, you say the problem is getting worse but you have no idea how big the problem might be?

Mr Henton: There was an IAM port (?) study in June 2006 that estimated that compromised computers send between 50 and 80% of all spam worldwide. My personal view is that it would be the top end of that estimate.

Q769 ***Lord May of Oxford:*** Could you convolve that with the number of things that are sources of spam to come to some sort of ball-park estimate of the number of computers thus compromised?
Mr Henton: We have not been able to estimate that.
Mr Blessing: Part of the issue is the fact that the traffic from those particular users is now not that different. Dr Clayton's work will help us spot some of that anomaly and we may be able to do some numbers.

Q770 ***Lord May of Oxford:*** It seems to me that the crunch question was going to be whose job is it to fix these machines but it now seems that the question is whose job is it to identify these machines and subsequently whose job is it to fix them? I find it interesting the fact that some of these things you seem to have made an almost evangelical virtue—and I can sympathise with it—of, "It is not my problem. I am just being creative. Do not interfere with me lest you screw it up." Do you not think it is somebody's responsibility to be thinking a little bit more coherently about some of these things? I am surprised that the answer to that question is, "I have no idea how many are compromised."
Mr Souter: I think we do know.

Q771 ***Lord May of Oxford:*** Good.
Mr Henton: I think the figure is very well-known. It is not talked about for the very reasons that you have just alluded do but I think a lot of large ISPs absolutely know.

Q772 ***Lord May of Oxford:*** What is it?
Mr Souter: You would have to get the collective figure from each of the ISPs to come up with a number and that is the unobtainable answer in response to your question. There is no doubt about the question.

Q773 ***Lord May of Oxford:*** If we were to ask could you follow up on that collectively to give us a written supplement, would that be a sensible question?
Mr Blessing: We could ask our members if they can give an estimate and feed those numbers back. I do not know how good the level of response you would get would be, but we can always ask.

Q774 ***Lord May of Oxford:*** I should not speak for the Committee but I think that in itself would be interesting, the two-fold numbers of what is the estimate made by those who responded and what is the percentage of those who were unwilling to respond. I think the Committee might be interested in that.
Mr Souter: I think that would be a fascinating answer. I think the trouble is in posing a question of this nature, inevitably what people are going to then do is to try and figure out why the question is being asked in the first place and what the implications are, and that will inevitably impact on their reply. We did some work on this in LINX a little while ago where we talked to only to a tiny, tiny subset of the very largest ISPs and the numbers that we are talking about are horrific. They are in the millions. Let us get that out on the table. This is slightly out-of-date information now because we did this survey a little while ago but there is no doubt that it is in the millions. Given that the most recent Ofcom figures show that there are 11 million consumers with broadband access in the UK (and that itself represents an under-estimate of the total number of PCs that are connected, it is a much bigger number than just the 11 million) then the proportion is pretty high. As Matt said, this is ever-changing because as people fix vulnerabilities those machines will disappear off the botnets and then they will be harvested again through some other new vulnerability. If there was a clear direction as to where we are going with this, then perhaps something productive might come out, but I suspect if you simply say, "What is the figure?" you can choose any scary figure you like.
Lord Mitchell: But you are the experts, you must have a feel for it?

Q775 ***Chairman:*** He has told us there are millions. Can we ask AOL how many machines do you communicate with that are compromised?
Ms de Stempel: I actually do not know but I will follow that up. I think it is a bit unfair to say that we are abdicating all responsibility. We are actually working very hard to push these network security items to all our consumers. We are trying to make people put an anti-virus on their machines. We are promoting this regularly and we are pushing it regularly. We are participating in Get Safe On-Line. We are participating to every single action that we can.

Q776 ***Lord May of Oxford:*** I may have put it too strongly. I guess to put it more fairly I would say the sense I get—and I may be alone in this—is collectively you seem to see a tension between creativity and accountability and my personal impression is that for at least to some of the answers the balance was tipped, for my taste, far too much towards the creativity rather than the accountability.
Mr Souter: I do not think that is the issue here. I do not think it is a tension between creativity and security/protection. I suspect it is an economic argument. If you think about what would be involved in the larger

networks, who clearly know they have got large numbers of compromised machines on their networks and what they could do about it and the cost of doing that. Matt gave an example there: imagine a multi-session telephone call with one particular user where you guide them through the process of getting their compromised machine back to a level where it is not compromised any more and it is fit to be on the network and then it is additionally protected such that it does not get immediately compromised again; imagine with someone who is not particularly expert how many telephone conversations that is going to take and just how difficult it would be to resource that on a scale of say a million, because we have got some networks in the UK that now have several million broadband access customers. I think therefore what you are talking about is an economic issue rather than something that is to do with the things that Malcolm was pointing out about the way the network is designed. We are talking about compromised end-user machines here, not something inherit in the network at all or to do with network creativity.

Q777 ***Chairman:*** I think we are going to have to move on. We are running very short of time. Just a couple more questions is all we will have time for. Would you welcome a breach notification law? Have there been cases of ISPs losing personal data?

Ms de Stempel: ISPA would not welcome the security breach notification law nor does it see the value in having one. There are already security co-ordination centres and we believe that joined-up industry action by the various sectors affected by threats to on-line security will be the only way to usefully combat on-line security threats. The wide range of industry participants involved in the GSOL from the communications, banking and security industries demonstrates that GSOL has already started to facilitate this, but while consumer awareness has been raised there is still a long way to go in changing consumer attitude. It is something that we are working very much with all other industries to raise consumer awareness as to what they should do.

Q778 ***Chairman:*** So you are saying that if an ISP loses all of their customers' data or some of their customers' personal data that they should not be held liable? The majority of US states now have breach notification laws.

Ms de Stempel: I read the question more as security as in someone attacking your system or being aware of a fake web page that purported to be what it was not, so maybe I am misunderstanding the question.

Mr Hutty: It is important to be clear here about whose security failure it is and who is doing the notification. If an ISP loses data properly under its control, like its customer account database, then it would already probably have infringed the Data Protection Act—that is one thing—but I am not aware that is really something that happens. I am certainly not aware that there is any clamour that that is a serious problem in that it happens a lot, so maybe you have some evidence or some instances of that of which I am unaware. I suspect where this is coming from is instead the concern over people who operate web sites, who run e-commerce sites, or who do other things on the Internet who suffer security breaches. The question has arisen, I believe, out of the proposal for the breach notification law that has been proposed by the European Commission in the Telecoms Regulatory Framework, proposing that the European legislator should include such a provision within the review of the Privacy Directive in the Regulatory Framework. The problem is that that Directive applies to public electronic communications networks and public electronic communications services, so it would not apply to people like the e- commerce sites that are not taking proper care of the data. It would only apply to someone like an ISP losing their account database but, as I say, I am not aware of evidence that that is actually a problem. Certainly that is not the motivating factor behind this proposal. One thing I would certainly suggest is that the Commission have made a technical error in that proposal in including that within the Privacy Directive in the Regulatory Framework when actually with the policy question that they are attempting to address there, whatever the merits or demerits of the notification law might be, the appropriate place for that would be in a revision of the Data Protection Directive where it would apply to all data controllers.

Chairman: I think we are going to have to end it there. It has been a very useful session and we are very grateful to you. I think we understand the complexity of this topic because we have seen a lot of evidence on the dark side of the net and just what is going on there. There are literally thousands and thousands of credit card numbers and personal security information being traded and it has to come from somewhere, and that is why we are probing to see what the sources of this are because it is not satisfactory in our minds just to step back from it and say it is so complex and the Net is so complex that we cannot do anything about it. In any case, thank you very much for your evidence and, please, if you think of anything additional write to us. We have still got time to include it in our report as we will be continuing for another two or three months. Thank you all very much indeed.

Memorandum by the Internet Telephony Services Providers' Association

1. The Internet Telephony Services Providers' Association (ITSPA) is the UK VoIP industry's trade body, representing over 80% of UK businesses involved with the supply of VoIP services to industry and residential customers within the UK. We act as the representative voice of the VoIP industry to Ofcom, the Home Office and the DTI, as well as to EU institutions. Internet industries are global, and consequently the regulation of them must aim to follow suit. ITSPA has members in Australia and Europe, and pays close attention to the development of VoIP regulatory frameworks on a worldwide basis in order to ensure that the UK Internet telephony industry is as harmonised as it can be with international developments.

2. ITSPA welcomes the Committee's inquiry on this subject and the Internet. By responding to this call for evidence ITSPA hopes to offer clarity on what Internet telephony providers in the UK are doing to promote personal Internet security, thereby giving the enquiry an informed base to work from.

3. ITSPA has recently met with the Cabinet Office, the Home Office and the Association of Chief Police Officers regarding issues of traceability, where ITSPA emphasised that members hold assurances of personal Internet security for customers as paramount.

4. ITSPA is committed to combating the threats to personal Internet safety presented by Internet telephony, but firmly believes that the VoIP (Voice over Internet Protocol) industry is only one part of an extremely broad sector obliged to formulate a response to such threats. Our response will focus on VoIP issues and so must not be viewed as a comprehensive discussion of personal security issues.

Defining the Problem

What is the nature of the security threat to private individuals? What new threats and trends are emerging and how are they identified?

5. The motivations to attack Internet telephony users are very similar to those associated with conventional phone attacks: to benefit financially via toll fraud or identity and information theft, and to gain notoriety, by disrupting service and inconveniencing users. Furthermore, as computers running VoIP software are more like computer than phone in structure they are also potentially vulnerable to the unauthorised access, privilege escalation and "system" misuse, viruses and worms, and denial of service attacks exploiting network protocols that are typical of networked computers.

6. Potential threats are identified by security companies and trade bodies like ITSPA, and communicated widely through both the trade press and mass media. ITSPA has identified three threats that are currently of particular concern; phone spam, "vishing" and CLI spoofing. However, although we take every care to acknowledge and protect against these risks, it is important to emphasise that none of them are currently creating significant problems for UK consumers.

7. Phone spam, sometimes known as SPIT (Spam over Internet Telephony), is not yet a major problem but it has nonetheless received a great deal of attention from VoIP providers and the trade press. VoIP systems, like other Internet applications such as e-mail, are susceptible to attack by telemarketers or phone system abusers who initiate unsolicited and unwanted communications. Unlike e-mail however, the technology to filter or block unwanted calls is potentially extremely complex.

8. A further worrying new trend is that increasingly cyber criminals are targeting home users with "vishing" attacks. Despite deriving the name from "phishing", an e-mail based scam, "vishing" is essentially a traditional telephony process made financially viable by new telephony technology. It uses VoIP to send a large number of calls to standard PSTN equipment using originating equipment that would have been prohibitively expensive in the past. The Committee should note that despite the wide exposure it receives, this problem is often covered in a misleading way by the media and it does not currently present a major worry to UK consumers.

9. ITSPA members have also noted the difficulties posed by CLI spoofing. CLI (Caller Line Identification) or Caller ID is made up of two separate entities: the calling number and the subscriber name. CLI spoofing is the practice of causing the telephone network to display a number on the recipient's caller ID display which is not that of the actual originating station; usually for nefarious purposes.

10. The problems posed by CLI spoofing are three-fold. It can be used to trick subscribers into calling expensive numbers by giving a caller ID the user does not recognise—encouraging them to ring back. This practice has become incredibly common in some countries, notably Japan. CLI is often used for caller identification, and there are public expectations to this effect. However, there are now web sites that allow anyone to make a call with any caller ID, making it impossible to use such data as a reputable identification source. Finally, there are issues posed by the frequent use of caller ID for authentication. Major mobile

companies until recently had voicemail systems which would allow access to voicemail based solely on a caller's CLI. Someone wishing to check someone else's voicemail simply had to call their mobile number with the caller ID set to be the same as the number they were calling, allowing them to obtain access without any further form of authentication. Although it is important caution is exercised on this issue, it is must be recognised that UK networks have traditionally strictly observed caller ID checking procedures. This is unlike the situation in the US where telecommunications companies have not validated caller ID on entry to the network from "end-user" connections for some time.

11. When new threats arise, ITSPA members can bring up concerns amongst its working groups and push the issue onto the agenda at Council meetings. This allows for discussion of preventive tactics and the development of a coherent industry solution to the problem. ITSPA has a technical working group where such concerns can be investigated at length and where the right technical experts can resolve the various problems. ITSPA members are also heavily involved in wider industry groups such as the NICC, which try to tackle the various concerns that affect the VoIP industry. CLI is an important part of the NICC agenda.

What is the scale of the problem? How are security breaches affecting the individual user detected and recorded?

12. The scale of the problem varies according to the particular threat discussed. Although phone spam is subject to much industry discussion, there is little evidence as yet of widespread difficulty. Vishing and CLI spoofing are a concern but not to the point where the industry is struggling to cope. With the VoIP market growing rapidly, ITSPA understands it is imperative that there is careful monitoring of security issues.

13. ITSPA has endeavoured to tackle these problems at the earliest possible stages, and in doing so has successfully mitigated the damage they have caused to VoIP users in the UK.

How well do users understand the nature of the threat?

14. ITSPA works tirelessly to ensure that there are high standards of consumer awareness and believes that its members have a responsibility in providing clear education for consumers and simple products for consumers to use to address the security threats that present themselves in the online world. However, users also have a responsibility to protect their computers and the equipment that they are using. There is evidence to suggest that because of the rapidity with which the nature of threats can change, the precise nature of some security risks are not comprehended by all users.

15. By working in a flexible self-regulatory environment, the VoIP industry is better placed than others to deal with the constant changes in the nascent Internet world. ITSPA is able to quickly assimilate the nature of potential industry risks and convey this information to customers, unburdened by potentially cumbersome external regulation.

Tackling the Problem

What can and should be done to provide greater computer security to private individuals? What, if any, are the potential concerns and trade-offs?

16. Although hardware and software both have very important roles to play in curtailing computer security risks, the importance of consumer knowledge cannot be over-emphasised. Many Internet crimes perpetrated via Internet telephony rely on consumers being fooled, rather than an attack on the computer or its software. Both vishing and CLI spoofing are avoidable difficulties. ITSPA suggests that making the public more motivated to act on security concerns is a crucial step in fighting Internet crime.

17. ITSPA notes that many UK ISPs have run specific campaigns promoting security information to the public. We are also encouraged by initiatives such as Get Safe Online, which has received widespread media coverage and should go some way to protecting consumers against Internet threats. ITSPA would like to see the Government continuing to support such actions, and persist in including industry sponsors from the communications sector in discussions with the Cabinet Office, DTI, SOCA and other relevant bodies or departments. We would also like to be involved in setting up similar initiatives for Internet telephony in the future if it were thought that such a step would help consumers.

18. ITSPA believes that it would be crucial for any campaign to focus closely on the ever-changing threat posed by Internet scams. Whilst initiatives that target specific difficulties would have a positive impact in the short-term, the adaptability of cyber-criminals makes it fair to assume that there would be no realistic quick

fix. Consequently, a program aiming to target Internet crime by changing consumer attitudes is likely to be successful in proportion to how entrenched the message of caution is on consumers. While awareness has been raised, there are still some steps that need to be taken.

What is the level of public awareness of the threat to computer security and how effective are current initiatives in changing attitudes and raising that awareness?

19. The public is generally increasingly aware of computer security threats, though more vulnerable members of society who are less exposed to the Internet are still at great risk. However, the major problem seems not to be simply lack of awareness, but of action. Recent statistics have suggested that only half of the consumers surveyed for the report said they would ignore "phishing" e-mail messages. Even more alarmingly, almost one in 25 said they would respond to an unsolicited e-mail about their online bank accounts. These figures are in response to a relatively established scam. ITSPA is concerned that new tactics like "vishing" may potentially have an even more destructive effect if not acted upon.

20. ITSPA believes that it is clear that much work remains to be done. Security initiatives should not only be considered in terms of raising awareness amongst sections of society who may not be as immersed in Internet culture, but also to encourage positive action on the part of all private users. ITSPA is extremely concerned that the prevailing attitude appears to not take proper account of security risks, and works hard with its members to ensure consumer attitudes are appropriate for the problems faced.

What factors may prevent private individuals from following appropriate security practices?

21. There is a series of factors that may constrain use of adequate security by private Internet users. The main problem seems to be the lack of impact industry initiatives designed to encourage use of appropriate security practices are having. Despite a number of high-profile company campaigns and a genuine wish amongst many consumers to learn more about computer protection, the majority remain ignorant as to where to turn and what to do to make their computers secure. This is not simply a function of the complexity inherent in computers but is also indicative of the ingenuity of Internet criminals making it difficult for many to follow rapid developments in hi-tech attacks.

Governance and Regulation

How effective are initiatives on IT governance in reducing security threats?

22. The UK Government has played an invaluable role in reducing security threats through various policy and advice initiatives, such the Get Safe Online scheme already mentioned.

23. ITSPA is optimistic that the upcoming Internet Governance Forum, which will discuss Security as one of its topics, will be a continuation of the positive impact government initiatives have had in developing personal Internet security.

How far do improvements in governance and regulation depend on international co-operation?

24. ITSPA is concerned by the recent Ofcom consultation into VoIP, which fails to account properly for the flexibility of Internet markets and the associated risks of over-regulating UK industry. The Internet is a truly global entity and consequently it is of great importance that any governance initiatives recognise this.

25. If regulation of the Internet is to be successful and worthwhile, it must be done in a spirit of international co-operation and harmonisation. ITSPA believes that Ofcom's measures will ultimately fail to make a positive impact because foreign providers can continue operating (within the UK) outside of the regulatory framework whilst the competitiveness of UK-based firms suffers. As previously mentioned ITSPA has members in Europe and Australia, with the latter adopting a considerable amount of the ITSPA Code of Practice as part of the national regulatory framework. We feel that this approach of co-operation and convergence between countries will ultimately create the healthiest markets and most suitable regulatory framework to govern them.

Is the regulatory framework for Internet services adequate?

26. ITSPA firmly believes that the current system of self-regulation in the VoIP industry is perfectly adequate for anticipating, identifying and communicating the risks associated with Internet crimes.

27. Although ITSPA has been in existence for less than two years, it has played a major role in ensuring that the VoIP industry has grown in a rapid but stable fashion. Not only have businesses been well placed to deal with security difficulties, they have also been successful commercially as a consequence of ITSPA membership.

28. ITSPA would also encourage the Committee to note that for the past 10 years the Internet industry as a whole in the UK has been a model example of self-regulatory success. A clear endorsement of the success of this framework is the approach to self-regulation adopted in the UK's Communications Act 2003 and applied by the UK's national regulatory authority, Ofcom.

29. Imposing external regulation would inevitably make the process of communicating security threats to customers a slower one. As speed is of the essence when dealing with online crime, ITSPA believes neither consumers nor the industry would gain from any change of framework being imposed.

What, if any, are the barriers to developing information security systems and standards and how can they be overcome?

30. ITSPA believes that to excessively regulate this area would create a barrier to developing information security systems and standards, and that a flexible approach is needed in order to be responsive to problems as they arise. Given that the current state of affairs, ITSPA would suggest that any change to the existing arrangement must be considered with extreme care to determine whether it would be truly necessary.

Examination of Witness

Witness: KIM THESIGER, Internet Telephony Service Providers' Association, examined.

Q779 ***Chairman:*** Lord Chelmsford, thank you very much for being here and I am sorry we have kept you waiting, we overran, but I think you have been in the room and seen what was going on.
Kim Thesiger: Absolutely.

Q780 ***Chairman:*** You understand this inquiry and what we are interested in so would you like for the record to please introduce yourself.
Kim Thesiger: My name is Viscount Chelmsford. I go generally by my family name Kim Thesiger. I am the co-Chairman of ITSPA which is the Internet Telephony Service Providers' Association. I also represent on the regulatory front an ITSP called TruePhone which offers a Voice over IP over mobile phone service.

Q781 ***Chairman:*** How many UK consumers are using Voice over IP systems and how rapidly is the market growing?
Kim Thesiger: I think the market is growing very rapidly. As such, it is very difficult to calculate at any one time how many UK consumers there are. Ofcom did a survey last August which estimated the number of UK voice users at 1.8 million. We think it is probably significantly more than that by this point. I think it is worth saying that the total number of 1.8 million users in the UK is made up of three substantially different types of Voice over IP consumer. On the one hand you have the computer-based services such as Skype, MSN and those kinds of services which allow you to make PC-to-PC calls or indeed, with Skype, PC-to-land line calls. Then you have services that are offered by ISPs. Orange would be a good example of that and BT are also offering Voice over IP services over their broadband infrastructure. Often in those cases consumers are unaware they are using a Voice over IP service. All they are aware of is that if they take Orange as a service provider then they get much cheaper telephony as part of that service. The fact that that telephony service is delivered over voice over IP is often unimportant and irrelevant to many of the consumers. They would not realise that it is being delivered by Voice over IP. Then I suppose there is a third group of users who are using pure Voice over IP services, by which I mean they may be getting their Internet service provision from a completely separate company from where they are getting their Voice over IP service provision. These tend to be more sophisticated customers who are looking around for the best possible range of services and prices from a range of specialist Voice over IP providers. Mostly this would be relevant to companies and there are an increasing number of companies that are now having Voice over IP telephone systems within their businesses, but there is a small number of consumers who also go for specialist Voice over IP services as well.
Chairman: Good, that is very useful. Lord Paul?

Q782 ***Lord Paul:*** We understand that VoIP systems do not currently offer 999 services. Why is this? How much of a problem is compliance with the legislation and regulation in this area for the industry?

Kim Thesiger: I do not know of a single ITSPA member who does not want to offer 999 services and would like to do so as soon as possible, but there are some significant regulatory and bureaucratic problems to actually offering 999 services for most of our members. I suppose the main issue for us is the linkage between the ability to offer 999 emergency service calls and having to be what is called a PATS provider. PATS is a particular type of regulation which has a more onerous level of regulatory hurdles that one must meet in order to comply fully with PATS. In principle, most ITSPA members do not have a problem with the idea of complying with PATS. However PATS is still very copper-centric and still includes a lot of regulation such as the requirement to offer customers printed phone directories and to offer operator services. It specifies a requirement to offer text services to disabled users which is based on the existing PSTN copper telephone service, for example. All of that we are in discussion with Ofcom about and we understand that Ofcom are looking at the exact PATS regulations and how those should be changed for a Voice over IP world and IP communication world. However, there is one overriding obligation within PATS that does cause us problems and that is the network integrity clause. In a copper-based PSTN world it was very clear what represented network integrity. In an IP-based world it is very unclear what represents network integrity, and the message that we are getting from Ofcom is you must decide yourselves whether you have network integrity or not. There are no guidelines to help us decide whether we have network integrity, so the situation at the moment is that we might decide okay, we think we have done enough that we have satisfied the network integrity clause but if at some point in the future there was a problem with the provision of, let us say, a 999 service Ofcom, could simply come back to us and say, "Actually you are wrong, we think that what you had was not network integrity and therefore you are in the wrong and therefore you are going to be a fined a great deal of money." So it is important for us that this network integrity clause is cleared up. I should say that although Ofcom's legal advice is that in order to offer 999 calls you must PATS-compliant, that is not the legal advice that ITSPA has been given by a number of its legal members, and indeed there are other EU countries that have decided that the ability to offer 999 calls is in the overriding interest to be offered and therefore they have decided that actually you do not have to be PATS compliant in order to offer 999 calls. ITSPA would very much like to have seen that position taken up by Ofcom. We continue to work very closely with Ofcom to try and make sure that we arrive at a position where all ITSPA members can offer 999 services as soon as possible.

Q783 ***Lord Paul:*** Thank you. In the United States Voice over IP services are able to offer 911 services. What are the key differences between the regulatory regimes in the two countries that allow this? Has the provision of 911 services led to any problems in the United States? How reliable is the Voice over IP system and how often do the services break down?
Kim Thesiger: In terms of the differences between the US 911 system and the UK 999 service, we are in a very advantageous position in the UK. 911 systems in the US are based either at the state level or often at the county level within each state and it is not unusual in the US for different counties within the same county to have different 911 procedures. So in the US it is a real minefield for Voice over IP providers and they have got to think about how they work literally not even in every state but how they work in several counties in that state. In the UK essentially we have two 999 providers—BT and what used to be Cable & Wireless—so we can provide all 999 services through to access points and, potentially, it is extremely easy for us to offer 999 services. There are ITSPA members who are already offering 999 services and so all of that is entirely possible to do. In terms of whether offering 999 services over Voice over IP is inherently less safe, clearly there are a number of our members who are reliant on the network that is carrying those Voice over IP calls. Some of our members both own the network and they own the Voice over IP customers. Other members own the Voice over IP customers and each of those customers is using a different Internet service provider. Generally these days the reliability of broadband services is becoming pretty high. I personally use what is now Virgin Media and I have never, certainly in the last seven years, had any problems at all in terms of service outage, but a 999 call delivered over Voice over IP can only be as reliable as the underlying network it is delivered on.

Q784 ***Earl of Erroll:*** How secure is Voice over IP? When you dial a number will you definitely get through to the person you intended to?
Kim Thesiger: In terms of the technology behind Voice over IP there is no absolutely no fundamental reason why you should not get through directly to the person that you are intending to get through to. SIP, which is the technology which underlies a lot of our members' infrastructure, is a well-developed dual technology and we do not see any problems with reliability in terms of connecting people to the right number. So from that point of view we think it is very reliable.

Q785 ***Earl of Erroll:*** Your written evidence draws attention to the threat of CLI spoofing. How prevalent is this? Are you seeing a growth in this kind of fraud?
Kim Thesiger: We are not, frankly, but we are very concerned about the possibility of CLI spoofing and we think that is a real and significant issue. We know of at least a couple of web sites which allow you to

enter a number and send a call to another user who will be presented with a number which is absolutely not your number. You could choose any number to present. Clearly ITSPA members are absolutely banned from doing this. If we ever found a member doing this they would be kicked out of ITSPA. ITSPA members will allow customers to present a different CSL but only if there is direct proof that they own that number. A typical example might be that a company would want all of its employees to present the switchboard number rather than their individual numbers, so there are legitimate uses for presenting a different CLI from the telephone that you are physically calling from, but you have got to be able to prove legally that you own that number. In terms of the UK we would very much like to see the authorities going after anybody who is offering CLI spoofing. We think that it is something that is very dangerous. In terms of CLI from abroad, the vast majority of calls coming from abroad currently do not carry any CLI and I think we would have to be very certain that the network that was sending that call was a legitimate network before we were prepared to forward a CLI coming from outside the UK.

Q786 ***Earl of Erroll:*** Although there is of course a terrible sanction of being thrown out of ITSPA, should there not in fact be more onerous sanctions because they can still continue in business but not as members of ITSPA.
Kim Thesiger: Absolutely. We cannot see any reason why anybody would offer a service offering people to spoof a CLI number. We would like to see that illegal and we would like to see action taken against anybody who offers it. As far as I am aware, there is no legislation which would allow the police to act on such people at this time.

Q787 ***Earl of Erroll:*** I know you were in the room when I asked that question about whether you could have combined man-in-the-middle attacks for phishing and vishing with the presence of VoIP so that in fact both channels of communication were compromised.
Kim Thesiger: I think anything is possible but in terms of VoIP, vishing is something that is slightly different. Any technology can be compromised but if you take some security measures then you should be able to protect against something like phishing, and really it is more about protecting the ITSP's infrastructure than it is about protecting the customers' infrastructure, and any reputable ITSP in this country would have taken strong steps to protect their own infrastructure because their business depends on it.

Q788 ***Chairman:*** Is Spam over Internet Telephony a problem? If it is, what is the industry doing about it?
Kim Thesiger: There has been a lot of the talk about Spam over Internet Telephony and there have been a lot of media reports about Spam over Internet Telephony. I would have to say at this time we have not seen any examples of it. We actually believe that because the cost of calling a telephone number over the ordinary PSTN is so low now that actually there is no greater threat for Voice over IP customers receiving unsolicited calls than there is for ordinary telephone customers receiving unsolicited calls. Voice over IP however does present a real concern in terms of unsolicited calls and tele-marketers, et cetera, and that is less that it enables them to make more calls more cheaply to customers but rather that it enables unscrupulous tele-marketers to set up and operate much more cheaply than they used to be able to do. If you look at the situation five or ten years ago, it would cost a tele-marketer tens of thousands of pounds to set up in business and get the correct machinery to enable them to use multiple ISDN lines, et cetera, to operate as a tele-marketer. What used to cost tens of thousands of pounds barely costs hundreds of pounds today. Somebody could set up in their back bedroom with a broadband connection and become a tele-marketer. We see that as really being the danger that Voice over IP brings to the unsolicited calls market. Obviously we are concerned about customers receiving tele-marketing calls or unsolicited calls but at the same time we think that the focus needs to be on stopping illegal tele-marketing calls from leaving our networks in the first place, and that is where we are putting the effort at the moment. There are certain customers that ITSPA members have which are legitimate and responsible tele-marketers. Equally, we are looking at solutions for them in which we can automatically check outgoing calls from those customers against the telephone preference list and make sure that they are not by mistake making any calls to a number that is on the telephone preference list. So we see really Voice over IP as posing an issue more to the generation of unsolicited calls rather than the reception of unsolicited calls.

Q789 ***Chairman:*** Getting back to vishing but also considering this SPIT problem, clearly your motivation in ITSPA is the correct one. You are paying attention to the benefits of the technology but do you think that customers will really get what they need? In other words, will the companies not just deliver the minimum level of security that they can get away with?
Kim Thesiger: Clearly there is that kind of concern, but we are a new industry and we realise that there is an awful lot of publicity about this industry and, if anything, ITSPA members have tended to be overcautious. I suppose one of the things that really gives me a lot of hope for the future is that for a very new

industry ITSPA was started up at the very beginning of that industry. I guess of the actual specific Voice over IP services rather than the PC-to-PC and PC-to-PSTN services like Skype and MSN we represent probably 80% or more of all the providers in this country who are offering Voice over IP services directly. The members have been very proactive about getting together, we have a very energetic technical working group who look at these exact kinds of problems and look at the solutions that we can apply to them. So I think we are only too aware of the reports in the media about the potential of vishing and SPIT, et cetera, and we are very, very keen to combat that and make sure that that does not become something that can be used against us in terms of the services that we are offering.

Q790 ***Chairman:*** A final question: what impact is ENUM going to have on personal privacy and security?
Kim Thesiger: We think ENUM has the potential to offer some issues in terms of privacy, but we also think it is very early days. There is still a lot of discussion that needs to take place in terms of ENUM. Many ITSPA members use ENUM but only on an internal basis within their networks where it does not have any implication whatsoever. We really believe proper public ENUM to be quite a long way off. We conceive of there being an awful lot of discussion before proper public ENUM is actually introduced. Clearly there are privacy issues and those privacy issues have already been an important consideration in the DTI's discussions about the future of ENUM, so one of the things that must be introduced in order for public ENUM to be introduced and to gain any sort of popularity will need to be for example protection against number redirection. Another thing that will clearly need to be introduced is to make sure that you cannot simply deduce all sorts of other information from an ENUM number. We actually think that even today it is difficult to deduce much from an ENUM number that you could not deduce from somebody's e-mail address. Somebody's e-mail address can often tell you which ISP they belong to, et cetera. So, yes, ENUM offers the potential for issues but there is a long way to go and a lot of discussions to be had before it becomes a real issue and we will certainly be wanting to make sure in those discussions that the privacy issues and the redirection issues are addressed.

Q791 ***Earl of Erroll:*** Will not ENUM be quite useful for getting through to people, so it would be sad to knock it on the head because we are over-concerned?
Kim Thesiger: Absolutely. Potentially ENUM is a very interesting and powerful tool which allows you to be contacted where you want to be contacted. The concern is that it is quite a top-down proposal and that the introduction of ENUM is likely to be quite slow and take quite a long time. Many ITSPA members are already offering the kind of benefits that ENUM could offer but within their own networks so, yes, we are engaged with ENUM, yes, we want to make sure the consumer is protected, but in fact there are other ways we can already offer some of the benefits that ENUM will offer through our own networks.

Q792 ***Chairman:*** Lord Chelmsford, thank you very much. That was clear and concise evidence and very useful to us.
Kim Thesiger: You are welcome, thank you very much.

WEDNESDAY 28 MARCH 2007

Present	Broers, L (Chairman)	Mitchell, L
	Erroll, E	O'Neill of Clackmannan, L
	Harris of Haringey, L	Paul, L
	Hilton of Eggardon, B	Young of Graffham, L
	Howie of Troon, L	

Examination of Witnesses

Witnesses: MARGARET HODGE, a Member of the House of Commons, Minister of State for Industry and the Regions, MR GEOFF SMITH, Head of e-Business and e-Security, Business Relations 2 Management Unit, Department of Trade and Industry, MR VERNON COAKER, a Member of the House of Commons, Parliamentary Under Secretary of State, and MR STEPHEN WEBB, Head of Organised and Financial Crime Unit, Home Office, examined.

Q793 ***Chairman:*** We are being broadcast and televised. Thank you very much, Ministers, for coming to help us in this inquiry, and Mr Smith and your colleague. We are fairly well into this inquiry into Personal Internet Security now, as you might be aware, so we appreciate it very much that you are coming to talk to us now and can answer some of our questions. Would you like to proceed by first of all introducing yourselves and then, if you wish, making an opening statement, or we can go straight into questions? Perhaps we could start with Mr Smith first.

Mr Smith: Thank you, Chairman. I am Geoff Smith, Deputy Director of Communications Policy in the Department of Trade and Industry.

Margaret Hodge: I am Margaret Hodge and I have ministerial responsibility in the DTI.

Mr Coaker: Good afternoon, Chairman. My name is Vernon Coaker and I am the Home Office minister with responsibility in this area.

Mr Webb: Good afternoon. Stephen Webb, Head of the Organised and Financial Crime Unit in the Home Office.

Margaret Hodge: The position is that we have not got an opening statement because we thought you would like to use the time to quiz us.

Q794 ***Chairman:*** Yes, we do have quite a long list of questions. I appreciate that. Let me go straight into the questions then. What is your estimate of the direct and indirect cost of Internet-related crime to the UK economy?

Mr Coaker: Chairman, I thought I would start with answering that question and I hope the Committee will bear with me because I thought it would be helpful if I lay out the statistics we have got. I thought it might be useful for the Committee's information to look at the actual statistics we have got at the present time. Could I just say that the police figures do not actually record the medium used to perpetrate the crime, only the offence committee, therefore online fraud will actually be recorded as fraud. I think that is just a statement to make in the first instance. In terms of direct losses, the most reliable figures we have got at the present time are from the 2003/4 British Crime Survey which we actually published in April 2006, which showed 27% of households with Internet access reported that their computers had been affected by a virus and a third of those reported that the virus had damaged their computer. Two per cent of households with Internet access reported that someone had accessed or hacked into files on their home computer in the previous 12 months. According to APACS, £154.5 million in card fraud losses took place over the Internet during 2006, and that figure is actually an increase of 32% from 2005, where the losses were £117 million. With respect to online banking fraud, in 2006 the losses were £33.5 million, which is an increase of 44% from 2005, where the figure was £23.2 million. Much of the increase has been driven by the increase in phishing incidents and if I tell you, you can actually see the increase. In 2005 the figure was actually 1,713 and that had risen last year to 14,156. Online banking fraud losses are smaller compared with plastic card fraud losses, which are as a whole £428 million, but as I say that is a considerable figure as well. I thought it would be of interest to the Committee as well to lay the statistics on the Chairman. APACS pointed out in the second half of the year enhancements to fraud prevention systems used by the banks to detect fraud actually were reflected in the figures, in that losses were greater in the first half of the year, at £22.5 million, than they were in the second half of the year, at £11 million, where the enhanced fraud prevention measures were put in place. I think that again, to be helpful to the Committee, shows the importance of the implementation of these measures and the effect and impact that can actually have when it comes to the prevention of crime. The latest research shows in the first half of 2006 16.9 million people used the Internet banking services in the UK. The last

statistical point, again trying to be helpful Chairman, is that the Office of Fair Trading estimated Internet dialler scams and Internet matrix scams cost the public a total of £70 million each year, but if we actually looked at scams where using the Internet plays only a part, for example an African advance fee fraud victim who may have been targeted using the Internet, if we included that the figure would be much higher. I apologise to the Committee for a bombardment of statistics, but I thought it would be helpful to share that statistical information with the Committee as far as we had got, Chairman.

Q795 ***Chairman:*** That is very useful. So in general you would say that the situation is getting worse rather than better, however there are some means being applied which are improving things?
Mr Coaker: I think it is fair to say that this is an increasing problem which we need to be aware of and also that the criminals who are using the Internet in order to perpetrate crime are also becoming increasingly sophisticated in the ways in which they are trying to attack the system. In a sense, Chairman, I think the best way of describing it is to say that what we essentially have are virtual criminal gangs. They are real people but they are acting in the virtual environment and there are online gangs, if you see what I mean, as well as individuals, and I think we are all becoming increasingly aware of the sophistication of the tactics they use. We have had some success, but increasingly we are going to need to develop the tools that we use against them in a more coordinated way in order to be as effective as possible.
Margaret Hodge: Could I just add a word of caution to all the statistics, which is that we have not got robust figures, so I do not think any of us have real confidence in the figures, and the sorts of issues which cause us to question them are that firstly, usage is going up, so if the figures go up are they going up proportionate to usage, and the other is that for some people in the industry there is a reputation issue, so we simply have to watch whether or not that gives us a true indication of whether people are reporting the crime. On the other hand, there may be more consumers, more end-users, who do have the confidence and therefore report crime. The only other bit of statistics I wanted to add is that Vernon does all the sorts of surveys around individuals and victims, and we do one with businesses where we talk to 1,000 businesses every two years and it is an information security breaches survey. That captures everything. It does not just look at crime, it can look at operational error and things like that as well, but the interesting things coming out of that survey, which we believe is quite comprehensive, are the indirect costs where you are trying to cost things like disruption and reputation. For a small business it is somewhere between 6,000 and 12,000 if there are one or two days of disruption. For a large business it is between 50,000 and 100,000. Then if you go to the direct costs what the companies tell us, 85% of them, is that there is no direct loss to them from crime, but those who have lost are the other 15%, the small companies. It is not a large amount, it is between 500 and 1,000, they report, and for large companies it is over 50,000.

Q796 ***Chairman:*** Presumably these are difficult to estimate? We have heard from people like eBay that they do suffer from this because every individual who has suffered fraud and who has been ripped off never comes back again. So it is a critical issue.
Mr Coaker: That is right.

Q797 ***Lord Young of Graffham:*** Unless I misheard, your first statistic was 27% of homeowners with computers on the Internet were infected by viruses. Is that the correct figure?
Mr Coaker: Yes.

Q798 ***Lord Young of Graffham:*** That is a remarkably high figure when you think of the proportion of people who have protection anywhere in their machine. Do you have confidence in the figure, that people are not just confusing that with a crashed hard drive or some other software fault and are saying, "We've been affected"?
Mr Coaker: I think that is an important point to make. As my fellow Minister was saying, it is very difficult. I just wanted to say that these are the ballpark statistical figures which we have. It is very difficult to know quite how robust those figures are because I think it is quite right to point out that it may well be just people where something has happened and they describe it as a virus affecting their computers. I think this is part of the problem as well, trying to get robust statistics together, but as I say I thought it was just necessary to say that these are the statistics as far as we have them. But it is an important point you make.
Margaret Hodge: It is very interesting, again, on viruses that in preparing for the Committee today there was one survey I came across which suggested that only 1% of those who were affected by a virus ever get to talking to the police about it, and a very small percentage, about 8%, even go to their service provider. That is also, on the virus issue, how people perceive and deal with breaches of the legislation.

Q799 ***Lord Howie of Troon:*** Since we will have to pay some attention to these statistics at some stage, can you tell me whether the robustness is an over-estimate or an underestimate, or you just do not know?

Margaret Hodge: We do not know.
Mr Coaker: The most reliable figures we have got, as I say, come from the British Crime Survey, which are the figures I have just used, about 27%. As I say, those are the ones who said they had been infected by any virus. If you actually then go on, just 2% reported that someone had tried to access or hack into files on their own computers. That is obviously a much lower figure. I think the BCS figures are the most reliable figures, but I think you can put a health warning on those, to be honest.
Mr Webb: The BCS figures are the best for total victimisation. The APACS figures which the Minister quoted are actually, we think, very robust. They are collected from the industry as a whole and we have got a lot of confidence in those.

Q800 ***Lord Mitchell:*** I am very surprised, perhaps delighted, that you say 16 million use online banking, that is one in three of the adult population?
Mr Coaker: Yes, 16.9 million.

Q801 ***Lord Mitchell:*** I am staggered by that. I would have thought it was much less.
Mr Coaker: These are APACS's figures and, as Stephen Webb has just said, we regard APACS's figures as very robust.

Q802 ***Lord Harris of Haringey:*** That is not the number of accounts, that is the number of individuals?
Mr Coaker: Yes, using Internet banking.

Q803 ***Lord O'Neill of Clackmannan:*** In terms of credit card transactions, do you make any distinction between chip and pin transactions and transactions involving telephone and the ones which involve broadband, because obviously there are different kinds and there are different security systems involved in them? Have you made any attempt to differentiate within credit transactions the various types and have you any evidence, for example, to tell us whether chip and pin has made a lot of difference in crime reduction?
Mr Webb: The APACS figures are broken down into a series of frauds and one of them is "card not present" and that would be quite a variety of crimes, including mail order over the phone but increasingly over the Internet. That is broken down and APACS's general point on "card not present" is that it has been increasing quite considerably, but they feel it has not been increasing as fast as the actual use of cards on the Internet and the use of Internet banking. So arguably the risk for any individual user has been declining and overall card fraud is obviously actually slightly declining too, which given the huge increase in the use of cards is again in real terms an improvement.

Q804 ***Lord Paul:*** The UK has not ratified the Council of Europe Cyber Crime Convention. Could you tell us why it has not been done, and if we are going to do it when it is likely to be done?
Mr Coaker: Yes. Thank you very much for that question, Lord Paul. We are committed to ratifying the Council of Europe Convention. We need to make some minor changes to the Computer Misuse Act, which until we have done that will actually delay the ratification. The minor changes we need to make to the Computer Misuse Act, the legislation, is actually contained in the Serious Crime Bill. That is obviously in the House of Lords at the present time and will come to us in due course, then that will be implemented and we will look to ratify that. We estimate that will be in about a year's time. We are committed to ratifying the Convention, it is just that there are some minor changes which we need to make to the legislation in order to do that.

Q805 ***Lord Paul:*** The Convention contains a number of provisions relating to mutual legal assistance and to the expedited handling of cross-border requests. Have any steps been taken to speed up the glacial speed at which MLA usually proceeds?
Mr Webb: This obviously goes a lot wider than the Convention. We have been generally looking at mutual legal assistance requests and there is nothing specific in this particular area which is being done. Therefore it is handled through the UK central authority.

Q806 ***Lord Paul:*** What procedures has the Government put in place for responding to complaints received from overseas?
Mr Coaker: I think we are looking to develop our whole system of reporting, whether it be from an international perspective or from the national perspective, which we may come on to later, and it is something which we need to consider, how we actually deal with that and do that.

Q807 ***Lord Paul:*** Is Europe far ahead of us in this?
Mr Coaker: From our estimation all countries are at various places and I do not think there is anybody who is a lot further on with this than we are. What is happening is that countries across not just Europe but across the globe are actually recognising the fact that if we are going to tackle this problem then we need international solutions and we need countries working together across the globe, frankly. What we need to do is, instead of trying to catch up with the criminals, to try and have a step change and move in front of them. As I say, there is a lot of work done on

it internationally, both with the Council of Europe and, as I understand it, the EU and other bodies as well.

Mr Smith: Could I just add to that? The European Commission has been telling us for some time that they are going to give us a communication on cyber crime[1]. It has been a long time delayed, but we have had a sort of peek behind the curtain last week and we think that it is going to say a lot about improving mutual legal assistance within the EU. So I think there is a new initiative underway on this front.

Q808 ***Lord O'Neill of Clackmannan:*** Would you support the development of a single UK or even England and Wales website for the reporting of cyber crime like there is in the FBI's US "IC3" website?

Mr Coaker: We have not come to any firm conclusions about this, but it is something that we are actually happy to look at in terms of the whole issue of reporting and how we do that. Obviously the Attorney-General and the Chief Secretary last week, in response to the fraud review, said that there was the possibility of the establishment of a national fraud reporting centre. We need to look at the whole issue of are we going to have a reporting portal for fraud, are we going to have a reporting portal for e-crime, or are we going to put all of that together? How would that work? How would you coordinate all of that? So I think there is a lot of work to be done, but the point is that there needs to be some coordination across the whole of this, so the answer is, we are looking at it and it is something we are considering.

Q809 ***Lord O'Neill of Clackmannan:*** One of the things we have come across repeatedly is that someone may get ripped off for a few hundred pounds, but there is every likelihood that simultaneously with that there is a whole range of people who have been robbed in exactly the same way. Should the police be trying to establish whether there is a lot of small crime rather than a big one, because at the end of the day as many people and as large sums could well be involved?

Mr Coaker: If you look at the law enforcement activity and the work which SOCA's e-crime unit is doing and some of the other activity which is being done, it is to try and piece together what on their own look to be small, individual crimes, to try and see if there is a pattern across the whole of the network that they can then piece together. I visited the SOCA e-crime unit recently to see that activity, where all sorts of reports were coming in and where they were trying to identify patterns of activity so that they can actually attack the criminals behind what, as you say, may be one small attack in a computer somewhere but if you take it across it would be thousands of £20 or tens of thousands of £15.

Q810 ***Chairman:*** Surely if you have a central reporting system you are going to learn an awful lot more because most people will not go to the police but, as has been shown in the United States, they will log their problem onto a website if there is a common website?

Mr Coaker: That is something, Chairman, we are certainly looking at because we are aware that that would be a positive move. What we are trying to understand is what is the best way of doing that when there are recommendations with respect to fraud, with respect to e-crime and all of that, and how you coordinate all of that activity and bring everyone together in a coordinated and coherent way.

Q811 ***Chairman:*** We are coming to the conclusion that there is quite a bit of urgency in this because at the moment even your statistics show that the overall level of this crime is relatively small and therefore there is a relatively small community there. Not that it is that small, and these people are clever, but as it rises that number is going to increase, you are going to attract more people to that and uncover unpleasant work, so we feel there is quite a deal of urgency.

Mr Coaker: We agree with that. What we want to do, however, is to move forward in a way which is actually manageable. If we set up without talking to all of the various partners involved, what we are concerned about is that the system almost may be swamped with people coming forward with possible problems and reporting potential fraud or losses, and the management of that data is actually then initially for the law enforcement agencies. We are not hostile to the idea and we recognise the urgency, but we want to do it in a way which is manageable and effective for the law enforcement agencies, so that it gives us the outcome we want.

Margaret Hodge: Can I come back on that because actually the challenge, even if the statistics are wrong—and it depends on how you identify the crime and which ones you are interested in—is that the level of crime relative to usage or ownership, or whatever it is, is pretty high. I think the difficulty with establishing that sort of framework or a legal framework is how you then, within that, with what will always be constrained resources, prioritise and target those crimes which create the most distress or loss, whatever it is, to individuals. That is the first thing and I think it is difficult. It is easy to say, "Have a website, have a law," but it is actually the implementation. You have got to be clear on the legislation. The only other thing I would say to you, which I know you and many of the Committee are

[1] Due on 22 May 2007.

highly aware of, is that this is such a vast changing industry with so much happening through convergence that actually framing a regulatory or legal framework which makes sense today and then becomes out of date tomorrow is just a difficulty that we have to think about all the time. So there has to be flexibility. You do not want to lock in a framework which then maybe stifles innovation, stifles change, and all those issues. So it is not quite as straightforward as putting up a website or introducing a new law, whichever it may be.

Q812 ***Earl of Erroll:*** The first thing is, how come SOCA is looking at this? It is not within SOCA's remit. SOCA only deals with crimes over £10 million or serious crime, so actually this whole question of level 2 crime which is perpetrated in small quantities but large volumes is not in the SOCA remit, so how come they were looking at it with you?
Mr Coaker: Because the point is that if you have got hundreds of small crimes occurring, it may be that if you look at the national picture you have actually got an international threat, because although they are small crimes individually the totality of it may be a serious crime.

Q813 ***Earl of Erroll:*** So are you thinking possibly of rolling the proposed, let us call it the national e-crime coordination unit, into SOCA as well?
Mr Coaker: What we are looking at—and again this is a moving picture—is that you have obviously got the SOCA e-crime unit and international and national strategic dealing with that level and what we need to look at is how we then co-ordinate, as you say, the level 2, the support for forces. I think, Chairman, you are about to see Commander Sue Wilkinson, and I have been talking to her with the Home Office about how we can deal with that as well.

Q814 ***Earl of Erroll:*** Are you going to give her resources?
Mr Coaker: We have not had the business case yet, so we need to look and see what proposals are coming forward from the ACPO lead on this and we will have to consider how we take that forward. We have made no commitment with resources at the present time, but it is something we need to look at and consider.

Q815 ***Earl of Erroll:*** So you might make e-crime a KPI and it can be measured and something can be done about it?
Mr Coaker: What we believe and understand is that we have got the SOCA e-crime unit dealing with it at that level, we are aware that individual police forces have been helped with funding since 2001 to develop their computer crime capacity in their individual forces, and then alongside that we need to establish how we coordinate the work at the ACPO level, which is something where we need to see how we take that forward and develop that. So it is not one strand or the other, it is all of those strands working together from the law enforcement point of view and the industry point of view in order to more effectively tackle this crime.
Chairman: That leads us on to Lord Young's question.

Q816 ***Lord Young of Graffham:*** Yes, which is really again for the Home Office. Do the police have adequate resources and even beyond that the right forensic skills to deal with cyber crime?
Mr Coaker: If you will forgive me for repeating a couple of the points in answer to Lord Erroll's question, what we have done, particularly since 2001 where over and above the police grant there were sums of money given to each of the police forces to develop their own individual force capacity, we have been working to try and develop the capacity of the forces to deal with e-crime in their own areas. We also recognise that alongside that there is a need to develop and look at how we have a nationally coordinated response, working above that at level 2, and we need to look at how we can take that forward. I think the issue with forensic skills, if I can be honest and speak personally about this, is a very real issue. When I actually went to the SOCA e-crime unit I looked at the skills of the people working in law enforcement there and I have to say I just thought it was just astonishing to see the abilities of people and what they were doing with computers from a law enforcement aspect in order to try and catch the criminals. I am not an expert when it comes to the Home Office policy remit with regard to trying to prevent crime, but when you actually look at the techniques and the technical ability which is required to actually prevent this crime, I am not sure how many people have that skill, certainly at the SOCA e-crime unit. These were fantastically qualified people. At a local police force level, I think obviously this is something we need to work on to develop with the police forces, and I think part of that will be working with industry as well.

Q817 ***Lord Young of Graffham:*** That really leads on to the next point I would like to make to you. In the United States the FBI have regional crime laboratories. Are we actually going to push it down to every single country police force, for every single police force in the country to set up its own laboratory, or are we actually going to look at it on a regional basis?
Mr Coaker: I think this is part of the ACPO proposals for the coordination of e-crime which we will actually have to look at, what would be the most effective way

of ensuring that every force has the capacity to deal with e-crime in their own area. Whether that is a regional type of approach or whether that is forces collaborating together I think is something we need to take professional advice on and, as I say, we are waiting for Commander Sue Wilkinson and others to come forward with the proposals.

Q818 ***Lord Young of Graffham:*** Traditional crime is regional. With traditional crime the villains are in the patch where the police are. We are not dealing with that. They can be in other parts of the world and it does seem to me a little bit odd if we are saying to Rutland, or to any police authority anywhere, "You've go to do your own," for something which is almost global.
Mr Coaker: I think that is right. What we are trying to do is to fill that protective services gap at an individual force level and how you do that will probably require a response which is above an individual police force, but I think what we have to do is to build confidence in communities across the country that e-crime is something which the law enforcement agencies, however they are configured and however they are set up to respond to it, are actually taking seriously and are actually trying to do something about.

Q819 ***Lord O'Neill of Clackmannan:*** We had evidence earlier from the Met which I think mirrored your confidence in their competence, but they also made the point to us that they lose a lot of people because they are so good and the City and others will recruit them, but we were also given evidence to suggest that there was a dependence upon special constables, who were in fact volunteers coming from City computer firms and the like who were doing this almost as a hobby. Are you satisfied that you have got the skill levels consistent with the increasing demands, or are you going to always be chasing them?
Mr Coaker: I think the forensic skill level necessary at an international level for ensuring that we have the capacity to deal with this, that individual forces have got somewhere they can go where they have the skill base necessary, is something which we need to look at and that, I think, will only come through collaboration and through working together. As I say, it is a developing picture but it is something which is crucial to us. I am not an expert when it comes to trying to work out what has happened with regard to computers, but we need the experts to help us if we are going to enforce the law effectively.

Q820 ***Lord Harris of Haringey:*** Following on from that, and I move on to my main question, we were told that the FBI has 300 forensic computer investigators, examiners. That suggests a scale of investment in this which is far in excess of anything which the police in the UK could muster. Do you agree that there needs to be a step change in the scale?
Mr Coaker: Certainly we need to look at how we are dealing with this crime across the country, and that is certainly what we are doing.

Q821 ***Lord Harris of Haringey:*** Mr Coaker, you have already told us that essentially there is no agreed definition of cyber crime, that most crimes are defined as broad or whatever else, but of course the consequence of that is that there is no policing target for investigating or prosecuting such crimes. Do you think the police should be set explicit targets for the investigation of cyber-enabled crime?
Mr Coaker: The whole question of targets is actually quite difficult because as part of the broader debate, Chairman, as you know, we are continually told to reduce targets for the police and not to constrain the activity of police forces and that they should be free to tackle crime as they feel appropriate. I would rather say, particularly as we are now in the process of negotiating a new set of measures and performance indicators for the police for April 2008, that the important thing to say is that all of us need to think of how we deal with e-crime and to actually ensure that it is mainstreamed into police work. I know the argument is that if you do not have it as a measure then it will not be mainstreamed. I have a bit more confidence about the future than that. I think the essential thing is, as I said, some sort of coordinated activity which goes on, that it goes down to the local police forces and that there is collaborative working and I think through that we will see a step change in activity across the country.

Q822 ***Lord Harris of Haringey:*** The Home Secretary, I think last week, announced that there would now be a special means of reporting crimes which involve a knife, and that slightly goes against your view that the police should be allowed to get on with it. Would there not be a similar case for saying that there should be separate recording of crimes which involve Internet use or computers?
Mr Coaker: Again, these are judgments which you make about how many targets you specifically have, what things you explicitly measure and what things you do not, but clearly the reduction of crime in all its forms will be a major part of police activity and certainly e-crime will be a major part of that.

Q823 ***Lord Harris of Haringey:*** In the absence, of course, of targets how are you going to ensure that resource levels are maintained, especially in terms of investigating level 2 crime which crosses force boundaries?

Mr Coaker: One will obviously be looking at the reduction of crime, the reduction of harm in communities, and the assessment which will take place in respect of that will be measured and as part of that process we will look to see how the police are doing in this area.

Q824 ***Lord Harris of Haringey:*** If I can just return to this question of aggregating crimes to create a big crime which is then investigated, we were told, I think on 21 February, by Gareth Griffith, who is the Head of Trust and Safety for eBay, "When we try to get police engaged, sometimes they say, 'Look, we'd love to help you. If it is not over "x" threshold'—thousands of pounds, or whatever it is—'we can't help you.'" Do you think that is an acceptable way for the police to respond to online fraud?
Mr Coaker: Obviously the police make operational decisions with respect to all crime, not just online crime. The police will determine what is an appropriate response with respect to anything which is reported to them. The point we have to make is that e-crime, online fraud, online crime is an important consideration for the police and they need to deal with that appropriately, but as I say there will be operational decisions which are made locally.

Q825 ***Lord Harris of Haringey:*** It is not something you feel the Home Office should itself monitor?
Mr Coaker: As I say, I think what we need to do is to say to the police that we expect the reduction of harm in communities to be at the forefront of their thinking, the reduction of crime in all its forms to be at the forefront of their thinking. They will be assessed, inspected and measured on that particular indicator and e-crime will be a part of that.

Q826 ***Earl of Erroll:*** We have been told by the police that the reporting procedures are going to change on 1 April and that the victims will be required to report the fraud in the first instance to the banks and no longer to the police, and then the banks will decide whether or not to report it to the police. What is the reason for this change?
Mr Coaker: We are actually trying to bring some clarity to the situation where we had before, in answer to Lord Harris's point, sometimes people going to the police with something and then the police saying, "Thank you very much for coming, but it is actually not something where we could go back to your bank." The Home Office, in discussion with APACS, looked at the situation and decided that the most appropriate way of (a) protecting individuals, (b) protecting business, and (c) actually giving us a better chance of actually catching the criminals was actually to have a more logical, rigorous system. So from 1 April people experiencing that sort of fraud, online fraud, will be asked to report that in the first instance to APACS, who will then make the decision whether to report it on to the police, because as I say people will go to them and will want what has happened to them put right and then APACS will get a bigger picture of what has happened and then report back to the police, who can then have a more intelligent overall picture of what is actually going on.

Q827 ***Earl of Erroll:*** Is there not a danger this will lead to a chronic under-reporting, because if the banks do not want to scare their customers then surely they have got a vested interest in not reporting it on to the police and just trying to play down the risks?
Mr Coaker: I suppose you could argue that, but the other argument would be that actually what people want is an effective way of tackling fraud, an effective way of tackling online crime, and if the Home Office, the banks, industry and business in general explain why it is being done then I think people will accept that, not as a way of massaging the crime figures but as an effective way of actually (a) trying to protect people, but (b) trying to get at the criminals who are actually behind the fraud which is being perpetrated on the individuals.

Q828 ***Earl of Erroll:*** We have heard that the banks are already not reporting fraud to the police directly, so why is this suddenly going to change? Are you doing anything to address the current under-reporting?
Mr Coaker: By actually encouraging people to go to APACS, I think we will get a better picture of what is actually taking place, because APACS will record that in their own figures and then we are saying to them, "Come to the police where appropriate." It is not about saying to them, "Don't come to us," it is about saying, "Then come to the police," but it will give us a better overall picture of what is actually taking place in the way that it will help us then to tackle crime.
Margaret Hodge: Can I help a little bit on this? If there is a filtering system, which is what this is, the hope is that those who do get reported to the police will be dealt with much more efficiently and effectively. One of the current problems is that people feel that if they do get to the police they do not get a response, and the banks themselves as a whole have told us and the Home Office that they do not bother, so if you can create a much more formal filtering system those who then get reported on to the police will be dealt with more efficiently and effectively. It is back to the fact that at present it is how you define your crime. At present it is like the British Crime Survey figures which looked at the virus. That might be the least

significant of crimes, but only 1% of people currently report those crimes to the police. There is an argument—and it is something the Committee no doubt will wish to consider—about which crimes should the police, with a limited finite resource, focus on. I think a filter is the sensible way forward.

Q829 ***Earl of Erroll:*** I can see, as you say, that it is a logical thing, but I wonder when the Federal Trades Commission in the States has gone the other way and said that you should report it first to the police, so that they have a sense of how much crime there is, and then it can be abrogated to the banks. So at least the police have a notion of really how bad it is, even if the banks are then going on to process it. Is that not a more sensible way to do it?
Margaret Hodge: That is a counter argument and my understanding—and I think probably Geoff will be able to expand on this, as I have not seen it first hand—is that actually operationally in the States, whilst this theoretically sounds a good model, it is pretty chaotic with pretty inconsistent outcomes for individuals.
Chairman: That is certainly not what we heard. We are looking at this from the point of view of the individual, not an efficient system which the state runs but from the point of view of the individual, and if you go to a bank very often it may be due to the bank's incompetence or even a problem within the bank, such as they have lost their data, which they have chosen not to tell people. What does the individual do? The individual can feel very threatened by this. You then go to somewhere like APACS, which tells you to go back to the bank. It may be that the bank is at fault. Think of the poor individual. The poor individual is now considerably worried and what we were told in the States is that what the individuals like is that once they have gone to the police they are given a standard form, and 18,000 police stations in the States have this form, and once you have filled that form out you at least have started down the road and you have declared that at least you are honest enough or that you have enough credibility that you go to the police and you have got the form filled out. The problem has still got to be dealt with, but I think to circulate the people back through the banks is just going to drive –

Q830 ***Baroness Hilton of Eggardon:*** It also protects the bank because it does mean that it is a proper claim and it is not someone pretending that someone has misused their credit card. So I would have thought the banks would welcome that. The other thing we saw was this excellent booklet which all police stations in America are given, which helps them deal with not just computer fraud but also the seizure of computers and how to preserve evidence, and so on. It was an absolutely excellent document, I thought, and something which without a great deal of resources the Home Office could actually implement in this country.
Mr Smith: We would be keen to have a look at that, Chairman.

Q831 ***Lord Harris of Haringey:*** It also runs contrary to the report produced by the National Consumer Council in this country, which says that the biggest problem for people in terms of sorting out identity theft is the fact that they cannot get ready access to crime numbers from the police and that they are shuffled backwards and forwards in a way which in fact is now being institutionalised.
Margaret Hodge: I think we should hear from the officials, but all I would say to you is that being given a crime number might give you a little bit of comfort, but if nothing happens beyond that I am not sure of the extent of the comfort you would get from that.
Lord Harris of Haringey: The National Consumer Council are saying that is what people need to sort it out.

Q832 ***Earl of Erroll:*** Anecdotally, a friend told me at lunch the other day that one of the things you are missing is that a lot of fraud is perpetrated by eBay and other auction houses, and of course they are not included in this, so where are they going to report it? This chap knew he had been ripped off for £100, he knew he was a sucker, he actually knew it when he was doing it, but what really upset him was not that he had lost £100 but that there was nowhere to report it. That is what really got his goat. At the end of the day you have got to have a reporting system to the police, I think, for the people outside. It is not just the banks and the credit cards, there is lots of other fraud going on there as well.
Mr Smith: I think you suggested that APACS might be interested in under-reporting. I simply do not believe that is true. I know you have taken evidence from APACS and I am sure they made that point to you strongly. They have no interest in doing that.

Q833 ***Earl of Erroll:*** They will only hear it if the bank tells them.
Mr Smith: I think Lord Broers made some very interesting points about certain types of crime where it might be appropriate to go initially to the police, but the statistics which we put out first abut the prevalence of phishing attacks I think actually argues strongly that you should go to the bank first, because it is essentially about in real-time stopping the money flowing, because if the bank is alerted very quickly then they can see the pattern of the phishing attack and they can start to take remedial action against the sites. As I understand it, the way they try and prevent

this is to try and stop the cash transfers and they try and limit the damage through that. So in a way, operationally the banks have got to come into this very, very quickly. I think that going to a police station, yes, it is great for getting a crime number and it is great for the back end of the process, but it puts delay into actually trying to solve it.

Q834 ***Earl of Erroll:*** Could it be done online, possibly?
Mr Smith: Yes. It takes us back to an earlier question about reporting. Could I just explain one last point, and I think it is a very pertinent point from Lord Harris about identity theft, which I think is a separate issue from the phishing attacks. I think a lot of people are realising that there are problems in that once you have lost your identity, where do you go to to get it reinstated? I know that the Crosby study on identity is looking very seriously at this issue and we expect them to report imminently. That may make some recommendations about that remediation process, and it is a very important point, I think, to address.

Q835 ***Lord O'Neill of Clackmannan:*** But there is a question of the independence of APACS because at the end of the day they are the creatures of the banks and on the insistence of the banks they will not even tell us which banks lose how much money. As a gatherer of statistics, I certainly do not have a great deal of confidence in them and I think you are giving them a degree of power and influence in them which hitherto their performance has not deserved.
Mr Webb: Can I say something about APACS and the crime statistics? You will have noted that all the statistics we gave at the beginning were from APACS's figures. In reality recorded crime figures on fraud have been very erratic and are not really that much help in understanding trends. Actually the point you make is a very interesting one. The fact that the banks know that their figures will not be quoted and broken down by institutions is why they have confidence in passing it on to APACS. If they thought they would get into the public domain then there would be those reputation issues, so I think that gives you more confidence in the figures. Just on the point about reporting to the banks as opposed to reporting to the police, of course anyone suffering cash, cheque or credit card fraud is going to go to the bank anyway, so what this basically means for the individual citizen who has been defrauded is that this removes from them the need to go to the police as well. It means also that the reports which will go from the banks to the police are more likely to spot the links. They are going to be a higher quality crime report than any isolated individual might be able to make and we would see this as reducing bureaucracy both for the police and also reducing burdens on the individual and I do not see any reason why APACS and the banks would not want to ensure this information did get across.

Q836 ***Lord O'Neill of Clackmannan:*** Mr Coaker, if someone comes to your surgery on a Friday or a Saturday and says, "I've been ripped off and I'm not happy with the bank that I'm dealing with. Could you tell me which bank I could go to, or alternatively where I can find out the relevant information which would give me confidence that the system the bank is running is better than some of the others?" at the moment you could not answer that question because APACS is not allowed by its members to make that information available. Do you not think, as a minister, you have a responsibility to the British public as much as to the ease of statistical collection and presentation?
Mr Coaker: What we are trying to do is to establish a system which more effectively tackles fraud and people being ripped off and having their money, or whatever, stolen online. The system we have put in place is about trying to protect the individual but also to try and pick up a pattern which may be established, which then means that we have got more opportunity to catch the criminals behind it. So what I would say to any constituent of mine is that the system we are trying to put in place is about trying to improve protection for them as individuals but also trying to give us a better intelligence picture, which will enable us then to get at the criminals who are behind that activity.

Q837 ***Lord Mitchell:*** Changing the direction of crime in some ways, on the subject of botnets we have seen evidence of the profusion of botnets for hire. The first question is, is it illegal to purchase the services of a botnet in the UK?
Mr Coaker: No, it is not illegal to actually purchase it. It is a difficult area because many computers, computer tools, et cetera, are actually capable of dual use. What is illegal is the making, adapting or supplying of articles for use in computer misuse offences. In the same way that knives can be used illegally but you would not ban all knives, that is in part the logic we are applying to this particular scenario as well.

Q838 ***Lord Mitchell:*** Does it make a difference whether the botnet is used for spamming or for launching denial of service attacks in terms of its legality?
Mr Webb: Purchasing is not an offence. Making, supplying or obtaining articles for use in computer misuse offences are, but not for purchasing.

Mr Coaker: The actual purchase is not illegal, but the actual use that you may make of an article is. If you make a particular article, if you adapt or supply an article which is subsequently then used in a computer misuse offence, that obviously is the part of it which is illegal. So it is the use you make of the equipment, or whatever, rather than the actual purchase of it.

Q839 ***Baroness Hilton of Eggardon:*** We used to technically deal with the proceedings around telephone calls by charging people for abstracting electricity. Presumably botnets are using people's electricity supply and technically, therefore, they could be charged with theft?
Mr Coaker: That is an interesting thought!

Q840 ***Chairman:*** You might argue that if the disk was activated in the computer when it would not otherwise have been activated you would be correct, would you not?
Mr Coaker: That is an interesting thought.
Margaret Hodge: But who would you charge?

Q841 ***Baroness Hilton of Eggardon:*** The person setting up the botnet?
Mr Coaker: If you could find them, yes.
Baroness Hilton of Eggardon: Certainly, that is if they are put in hundreds of thousands of people's computers.

Q842 ***Earl of Erroll:*** Surely if launching a denial of services attack is illegal, which it now is, then for conspiring to do so or purchasing software with the intention you could get them under some form of conspiracy act?
Mr Coaker: You could, yes, I think.
Mr Webb: What we do not have is a blanket offence for buying or possessing them. If there is criminal intent involved, certainly that would be.

Q843 ***Chairman:*** I would have thought it would be a positive move to make it illegal to collect together enough computers to have a substantial botnet unless you had a licence so to do. If you are doing it because you want to make calculations on climate, then you might have a licence to do it. We will get onto other questions about people who actually explore the security of the networks, but to allow people to hire out the use of a botnet to inconvenience everybody, if not to defeat service on the Internet, I would have thought should be illegal.
Mr Coaker: Chairman, let us write to you about that. It is an interesting point. We are trying to capture the criminality by the use of the computer facility, the computer hardware, software, or whatever. We are trying to capture the criminality through its use or supply, or the adaptation, but in part the point of committees like this is to reflect on points which people make, so let us reflect on that and write to you on that particular point to see whether we can move forward.
Mr Webb: Even with the law as it stands, the computer industry has concerns that it is potentially criminalising legitimate use.

Q844 ***Chairman:*** I think one of the points to consider is that the person running the botnet may well be in Eastern Europe, so if somebody is caught here transferring money via their credit card, or however, to somebody in Eastern Europe who is operating a botnet which operates with half a million computers in the UK then one should be able to go after that person.
Mr Coaker: It is an important point, though, Chairman, that the industry is concerned about the whole operation of dual usage and we do need to be proportionate and make sure that we allow legitimate business to carry on in an effective way. That is not to say that we do that in a way which means that we cannot tackle criminality, but we have been very effectively working with industry and we need to carry on with that self-regulatory and productive approach.

Q845 ***Lord Young of Graffham:*** It is a legal business to sell knives in this country if they are part of a dining room set, or something of that sort, but it is illegal if you are selling knives knowing that they are going to be used for criminal purposes.
Mr Coaker: That is a similar thing that we are trying to do with respect to computers.

Q846 ***Lord Young of Graffham:*** But a botnet would be the same thing if it is actually being hired out to somebody.
Mr Coaker: Yes, but that is the use of the system rather than the actual network.

Q847 ***Lord Young of Graffham:*** Yes, it is the *mens rea*. It is the intention in fact?
Mr Coaker: Yes.

Q848 ***Lord Harris of Haringey:*** Do you have a record of the number of incidents there have been for people using botnets illegally?
Mr Coaker: Again, Chairman, we can look into that, but I do not have it here. It might be useful if we write to you and you could circulate that to the Committee, if that is helpful.
Mr Smith: I think it is almost impossible to measure that in the UK, but there are industry commentators such as Symantec who do research into this and observe the development and use of botnets, and we can certainly provide information to you on that.

Q849 ***Lord Howie of Troon:*** Changing the subject a little, you will be aware, I am sure, that there are security breach notification laws in California and 30 or so states nearby. Have you any views on this? Would you like to see such things here?
Margaret Hodge: I am aware of that particular bit of legislation and clearly if somebody has their identity stolen there ought to be a right of notification. It looks an enticing bit of legislation. We are looking at it and Europe is looking at it, and Europe might well come forward as part of the review of the electronic communications framework, which I think we are expecting in about July. They may well come forward with a proposition around this area. I would simply draw to the Committee's attention what I am sure you have already thought of, which is the difficulty of framing that intent in a practical way because you would have to decide what breaches would you report precisely, what is the trigger for a report, those sorts of issues, and you do not want to end up in a situation where people either become really blasé about it because they get so many reports of breaches or they become so scared that they do not take advantage of the new information communication technology. On that latter point, we already know that actually people's fear of these sorts of crimes—and I was surprised to see this statistic—is much greater than their fear of muggings or burglary. So there is quite a lot of fear around this and we do not want that to be something which leads to exclusion from all the benefits which information communication technology developments b ring individuals. It is an interesting bit of legislation. We need to examine it. The devil is in the detail and we will think about it and look at what Europe brings forward in the summer.

Q850 ***Lord Howie of Troon:*** You say you are looking into it. I seem to have heard that several times during this session, you are looking into this, you are looking into that and you are looking into the other thing. Have you seen anything yet that is helpful?
Margaret Hodge: I think we are doing things which are helpful in trying to curtail crime and that surround, working with the industries so that they are better at the technology to ensure that they prevent it happening in the first place. What Vernon has been talking to you about is that there is a huge amount of activity in trying to detect it. I suppose the other thing which we jointly do is that a lot of effort goes into providing education and information to individuals so that they get smarter at using technology. Phishing is a classic example. If we did not give away our bank details so readily online our behaviour could immediately halt it and wipe out one area of cyber crime.

Q851 ***Lord Howie of Troon:*** You mentioned a proposal from the European Union. As we understand it, they would likely restrict notification to just telecom companies. Do you think that is adequate?
Margaret Hodge: What they have said, as I understand it, and I might defer to Geoff on this, is that they will use national regulatory authorities (which in our case would be Ofcom) as the regulator, but I do not think there is a restriction as to who would report through to Ofcom.
Mr Smith: That is absolutely a very fair point. In the US it is applied to all businesses and what the European Commission is saying, through the framework review proposal, is that this kind of legislation might apply to communications providers, which would be telecoms companies and ISPs. It looks slightly odd on the face of it to only be applying this kind of legislation to those providers and we could have the oddity of eBay or Amazon not being impacted by the legislation while Yahoo and Orange would be. This has to be seen, I guess, as a kind of transitory solution. It does show that European thinking is moving along the same lines as the US, but the US experience—I do not know whether you gathered this when you went to the States—has not been happy. I think the profusion of different legislations with different requirements has made a lot of lawyers rich, but I am not sure that it has actually increased security or increased consumer confidence. I fully accept the point the Minister has made. It is an interesting idea, but we have got to get it right.

Q852 ***Lord Harris of Haringey:*** We were advised that one of the problems was because there was separate legislation in 30 different states. Presumably that is not something you are envisaging. But we were also told one of the real benefits of this was that because of the reputational impact this has on companies the result has been that they take breaches in information security, whether it is a lost laptop or messy access to their IT systems, much more seriously and it has raised it up the agenda as far as they are concerned. That, presumably, must have a beneficial impact.
Margaret Hodge: It should be, but the danger of that is that you over-report and then you are into what levels should you be reporting to maintain confidence in people using IT generally as part of their lives, or do you over-report and then you become so blasé that they take none of it seriously? That is why the devil is in the detail of how you would frame this.
Lord Harris of Haringey: I do not think anyone was suggesting to us that there had been a negative effect on e-commerce as a result of the breaches.

Chairman: I think that is right, but they did say that the impact fell after a time.
Lord Harris of Haringey: As far as individuals were concerned, yes.

Q853 ***Chairman:*** That is correct, and so one has got to be careful not to report too much, as you say. But just having it in the background we think is very valuable in any case.
Margaret Hodge: Yes.

Q854 ***Baroness Hilton of Eggardon:*** If we can revert to the protection of individuals and whether the IT community industry should be doing more to look after people and prevent security breaches, do you think that would be beneficial? They kept talking to us about end-user agreements and flexibility of the system and all those other things they feel they should retain, but we were feeling that the people in between, the people who devised the software, the ISPs and so on, could do more to protect individuals. Would you agree?
Margaret Hodge: You mean should we encourage them or should we coerce them?

Q855 ***Baroness Hilton of Eggardon:*** Either.
Margaret Hodge: On the encouragement, self-regulatory front, I think we would be 100% for that. There is progress in where we are today compared with where we were a year ago or five years ago. If you look at the mechanisms now that we have got for filtering spam or checking for viruses, it is all much better today than it was a few years back. We do encourage—and we do it actually through the DTI by getting partnerships between our knowledge transfer network partnerships, which bring together all the key stakeholders from academia through to industry players across the industry through to consumers, the whole lot, and they share information and knowledge and also then can access various technology research pots of money to try and work in that area. I think we ought to do more. The more we can encourage, the more we should. The only thing I would add is the point I have made before, which is that just as important is the education of consumers, which is why our Get Safe Online efforts I think, are pretty important. We probably ought to be doing more to support consumers in using their technology sensibly.

Q856 ***Baroness Hilton of Eggardon:*** What about protecting consumers by providing them with more information when they get new computers? There is all this talk about firewalls and a various range of vocabulary which perhaps people do not understand.
Margaret Hodge: I can tell you that as a minister you have difficulty!

Q857 ***Baroness Hilton of Eggardon:*** That new patches need to be put on the software, and so on. That is all Greek to people and I think perhaps some simple instructions to people which went with their new computer could be helpful.
Margaret Hodge: Before we came into the Committee hearing today I was so amazed somebody on the Committee knows, but how we ever got to "phishing" with a "ph" I do not know.

Q858 ***Lord Howie of Troon:*** Indeed, I have often wondered!
Margaret Hodge: That is the sort of technological obscuration which I do not think helps anybody and acronyms in this world are also very difficult. I suppose the only other thing I would say about ISPs doing more and the industry making a greater effort—I have talked about what we do at home—this is also an area where we need to cooperate, not just in Europe but globally because that is absolutely vital in combating fraud.

Q859 ***Chairman:*** What about regulation which requires sellers with computers to state the condition in terms of time of their protective software, so that if you have got a computer which has just not been updated for six months with the latest viruses then it should state it like an out of date litre of milk, that this product is out of date, it is past its sell-by date? Why do we not do that?
Margaret Hodge: That is an idea which I think is worth exploring. What it presumes is that people know what they are buying. I have not looked at it in this area, but I am looking quite carefully at the moment as we go for digital switch-over at consumer knowledge as they purchase new televisions to cope with the switch-over and I think there is a huge lack of knowledge—with the sales staff also, interestingly enough, not just consumers—as to what software they are purchasing. So it is a good idea, but it has got to be part of a bigger picture is probably what I would say to you on that.

Q860 ***Baroness Hilton of Eggardon:*** The problem with the sales staff is that they glory in the complicated vocabulary, do they not, when they are talking to you?
Margaret Hodge: Or the turnover is huge. What we have tried to do on digital switch-over, which one could do anywhere, is to do a kite marking scheme for the retailers and for the producers as well, and that is always quite a good way of trying to get self-regulation to some agreed standard across industry. You can spread that sort of mechanism in any bit of the sector you want.

Mr Smith: Could I just add, the more consumers are working in a kind of "point and shoot" environment the happier I think everyone would feel and I think with the advent of broadband the automatic patching and updating of software actually has moved on considerably. To answer Lord Broers's point about the outdated software, most computers are now sold packaged with antivirus software. Admittedly, the package that is on the machine could be the 2005 edition, but when it makes connection, when you load it up, it will go to the website and update itself. If it is 2005 it will take for ever to update, but it will do it, so I am not so sure that is a big problem, but we will think about it.

Q861 ***Lord Young of Graffham:*** I have quite a straightforward question really. If a bank has a forged cheque from my cheque book it honours it. If my credit card gets stolen and I have notified the bank, and somebody else has signed it, they honour it. Should the banks be responsible for losses due to Internet fraud?
Margaret Hodge: You said it was a straightforward question. I wish I could give you a straightforward answer, because it depends on the particular circumstances, the particular fraud which has been perpetrated. So if there is a contract between the individual and the bank in that instance, the contract would determine who pays if something goes wrong. There is the banking code, which you will be very familiar with, which is basically that where it is believed that users took all reasonable steps to ensure that they would not lose their card then the bank will pick up the tab. I think you have established a liability. Liability exists in that context. I think that laying down absolutely firmly whose liability it is and when goes back again to the discourse we have had this afternoon about this partnership between the user, the provider and the banks. It is a difficult one. Who do you say is liable? I suppose our focus on that is working with the banks to ensure that they have better security. There is this new system, which I have not seen but I have heard of, where you have a different number on every transaction. What is it called?
Mr Smith: A one time password.
Margaret Hodge: A one time password, another terminology, so that every time you undertake a transaction you have that as security and that appears to be an improvement.

Q862 ***Lord Young of Graffham:*** The reason why I think there is more in this question than a simple answer is that we have moved in a progression from a world in which we all signed cheques and went into a bank to collect money to a world of ATM machines, and that will pass and we will be in a world in which money will be electronically transferred literally from my wallet to the bank. In those circumstances, should not either the DTI or the Home Office be looking very closely at the sort of regulations which could pertain to that before it begins to arise?
Margaret Hodge: It is a fast-changing world, so of course it is absolutely right that we should constantly be vigilant and ensure that the regulatory framework is appropriate, and actually in this instance probably it is the FSA rather than either of us here who would have responsibility.
Mr Webb: It is possibly worth also saying that there is currently a scheme verified by Visa and Mastercard of a secure code where, providing you as an individual sign up and the retailer signs up, you have a secure site where you can do your transaction and then that will be firm and the bank will stand behind that. So in a sense there is already the possibility for consumers and retailers to get into a position where the bank will guarantee the transaction. It is a relatively new scheme and the take-up is increasing but it is still relatively low at the moment, but that is certainly one of the things which APACS and the banking industry see as the way forward.
Mr Coaker: It goes back to Lady Hilton's point about the need for consumers to be aware of these sorts of things as well. Consumer awareness I think is a huge issue.
Lord Young of Graffham: Yes, absolutely.

Q863 ***Lord Harris of Haringey:*** If you really want to encourage e-commerce and you really want to encourage the banks to improve their security systems, requiring them to accept liability—as they do, I think, in the United States—for problems with Internet banking would surely be the most powerful driver of all?
Margaret Hodge: I think the answer is that that sounds easy, but then you have got to define the circumstances in which you would expect them to accept liability.
Lord Mitchell: The Americans seem to do so.

Q864 ***Earl of Erroll:*** Surely, it is the same as the Bills of Exchange Act 1886 or the American Regulation E, you just quite clearly put the liability on the banks? At the end of the day, they are the ones who control the money flow. Under the Bills of Exchange Act 1886 they had liability for a forged signature, or whatever, because there was a problem in those days. What we have now is an electronic way for them to offload that liability to the merchant or to the customer and we need to put it back with them, because they are actually the ones who could implement technology. If you look, for instance, at Alliance & Leicester, who have now

been authenticating their site back to their users for some time, they only have 0.01% of the Internet fraud, and the fact that the rest are hiding behind APACS because they are not implementing two-way authentication is an excuse. The things you talk about, actually two factor authentication, merely helps the bank not the consumer and the banks are hiding. If you put the liability back with the banks they will do something about it and all you need is some primary legislation to enable that to happen.
Margaret Hodge: I hear that and I think defining that primary legislation is much more difficult and much more complex for it to be fair than I think you have suggested in saying that to me. There will be some circumstances where we could put in primary legislation and there could be other circumstances where it is consumer behaviour rather than the banks which is at fault, which has led to a fraud or an abuse, or loss of money, whatever it is, a theft, and it is difficult to get those parameters right. What I do agree with you, and it is what we are trying to do all the time, is to try and improve the abuse of fraud by authentication schemes and working with the banks in that regard. We can go with the heavy hand of the law rather than the more self-regulatory route down which we are tending to travel and it is a matter of judgment for this Committee which it thinks is more appropriate. I leave that to you. We think we have got the balance about right, but you may think that we ought to be a bit tougher than we have been so far.
Chairman: We will go on discussing that, but I think we are minded to think that as things change more should be done.

Q865 ***Lord Paul:*** Can I ask a more simple question: who regulates Internet services in the United Kingdom?
Margaret Hodge: This question I had some idea you might ask. It comes from the idea that again it would be easier and simpler to have one regulator and one form of regulation. We are regulated by EU law, by UK law, and we also look at rather more global protocols which determine what we do. What we try to do in our regulatory framework is to ensure that the authority responsible for regulation offline is also responsible for regulation online. So the FSA, for example, will be responsible for online banking regulation. The main bodies we have got are Ofcom and the Information Commissioner, and I suppose a crude division of labour between them is that Ofcom regulates the industry—it is a bit too crude to put it like this, but I will say it anyway—and the Information Commissioner will look after the interests of the individual.

Q866 ***Lord Paul:*** We understand that by virtue of Section 32 of the Communications Act 2003 Ofcom does not have any remit to regulate the content that is provided via Internet services, but given the increasing use of the Internet to transmit content, which will accelerate with convergence, is this position tenable in the long term?
Margaret Hodge: Content on the Internet is extremely difficult to regulate because it does not get produced nationally, it gets produced globally. We are quite proud actually of the work led by the Home Office and led by Vernon Coaker around self-regulation on content, particularly in relation to child abuse and those sorts of issues. We have the Internet Watch Foundation, but it is extremely difficult to think of a mechanism which we implement nationally which would impact in the way we would want on what is a global service. That is really the problem we face. Again, if the Committee comes up with useful suggestions in that regard I think both the Home Office and the DTI would love to hear them.

Q867 ***Lord Young of Graffham:*** And the Government of China! You can access anywhere on the Internet but you cannot regulate, you simply cannot, as I have said. There are some governments around the world which have tried and have failed.
Mr Coaker: It is China I was thinking of.
Margaret Hodge: I was in China last October, where we talked a lot about how they could police their system rather better than they currently do, and they are making efforts there. There is actually a huge amount which comes from there, and from the States as well, which from your visit you believe to have a far better, stronger regulatory framework.

Q868 ***Lord Paul:*** Ofcom has statutory duties both to promote "media literacy" and to "conduct research" into such areas as "the experiences of the consumers in the markets for electronic communications services". Could Ofcom use these powers more proactively than it has done so far, in order to encourage better self-regulation within the industry? Let me give an example. What is the Government or Ofcom doing to persuade social networking sites such as MySpace to present appropriate guidance to users about the risks of disclosing personal information online?
Margaret Hodge: Could we have a step change in Ofcom's performance around its media literacy duties? I think the answer has to be, yes, and they are actually tackling that as we go. I am not quite sure where we have got to. They have produced an outline policy paper, which is probably out to consultation. I shall be corrected if I am wrong on this, but I think that is where we are, and that is coming back soon to them. But I agree with you entirely that they have a

role to play, amongst others, in providing much, much better education and understanding of the potentials and the dangers of the changing content in ICT, so absolutely, I am with that.

Q869 ***Lord Mitchell:*** You mentioned child abuse and I would like to come on to that subject. ISPs are being made to purchase and install systems to block access to child abuse image sites. The ISPs told us that this will not prevent the determined from accessing this material and will only prevent inadvertent access. Is there any evidence that inadvertent access to child abuse images is a significant problem?
Mr Coaker: There is no evidence about that being a problem. The last point to make about inadvertent access is that we have no evidence that that is problem, but I think it is a very important part of the Government's strategy in actually trying to prevent child abuse images being available on websites in this country. I think that the public would expect us to do everything we can to block these images. I am assured that there are people out there who have the technical ability to probably overcome the blocking processes which ISPs are putting in place and will put in place. Could I just put on record, Chairman, that I have been very pleased with the cooperation from ISPs in this area. There is significant blocking taking place already. I think that is a reasonable request to make of ISPs and I think the fact that some people may actually be able to overcome that blocking process is not a reason for it not to happen and in fact it is simply another hoop, if you like, which you put in place in order to try and protect the children of this country. I think that is a reasonable thing to be in place and I think most people would expect it to be there. It is not a magic solution. It is not a solution which says that if this is in place it will prevent any person from accessing these sites who are determined to do so, but it hopefully makes it much more difficult and hopefully, therefore, when it is brought to court the fact that somebody has had a particular technical expertise in order to access that site will help the court in determining the verdict.

Q870 ***Lord Mitchell:*** Do you not feel that it would better to push the responsibility for blocking content onto the end-user machine? Let me just add to that, in the evidence we have received it is staggering, for example, the lack of knowledge by parents on subjects like grooming sites, blogging sites, chat rooms and all the other things which go on. I think only 10% of parents were totally aware of what is actually happening on the Internet. What strikes us is that really when somebody turns on a machine for the first time there should be an access point actually telling people what the problems are. Just to give you a simple example, every time I turn on my car on the display it tells me not to look at the display when I am driving. It seems pretty obvious, but it is telling me not to do that and I do not see why, when people turn on their computers for the first time, it should not say, "We want to take you through all the dangers of the Internet, what you as parents should be aware of and what precautions you should take."
Mr Coaker: Certainly all of these types of procedures and processes we are looking at. We recently are looking at the BSI kite mark, which will be available for machines and software in order to show which are particularly good at protecting children or others with that particular piece of software or hardware. One of the things we are trying to prevent is the situation where you have a computer where the end-user has got a particular piece of kit which, when it is installed, will prevent them from accessing these abuse images, but I guess then you would have a situation where it could be uninstalled. It may be that just simply having an end-user product of some sort which will prevent access to child abuse images which is currently on the computer, and you sell it as such, and then somebody may uninstall it, so you have still got a problem with that type of situation where somebody who is determined to overcome it could actually do so. We think it is one way of trying to prevent access to child abuse images. We are moving towards a point where we have virtual total compliance, as far as is possible. If there are other processes that we can adopt at the same time, then I think we will look at those as well, but blocking is an integral part of that.

Q871 ***Lord Mitchell:*** I think education is an absolutely important part as well.
Mr Coaker: Yes, of course. That is a very good point and I should have mentioned that in responding to the question you put. You are absolutely right, education is an important part of this. It is like many policies in respect of this area, that actually it is not either/or, it is a combination of all of the various policies and a combination of all of these various factors in order to do what we all want, which is actually to protect our children.

Q872 ***Chairman:*** Let me move on to another topic. During our investigations we have seen a fairly large volume of illegal trading which is going on on the Internet of credit card numbers, credit card data, addresses, security numbers, et cetera. Bearing this in mind, is it any longer appropriate to pursue police investigations or still less launch prosecutions on the basis only of logs of credit card use?
Mr Coaker: Chairman, clearly much of the answer to that is operationally for the police. I think Mr Gamble gave evidence in respect of this matter. I

would simply make the point that I do not think the police would prosecute someone simply on the basis of their credit card being used. I think an investigation into whether you prosecute would require you to take account of all of the various relevant issues with respect to that particular crime which you were investigating. Of course, at the end of the day the evidence that you present would be tested not only by the police but by the Crown Prosecution Service and ultimately in the end by the courts to determine whether a crime had been committed or not. As I say, I believe that just on the basis of a credit card I am not sure the prosecution would proceed.

Q873 ***Chairman:*** Do you think they are sufficiently aware of this?
Mr Coaker: I think they are and, as I say, at the end of the day the great safety net for us all is the fact that the police made their investigations. That then has the test of the Crown Prosecution Service to determine whether they should prosecute or proceed, or not, and then ultimately it is a matter for the courts. As I say, many of these are operational matters, but I would be surprised if it was purely and simply on the basis of credit card details that a prosecution was taken forward.

Q874 ***Earl of Erroll:*** Regulation 5 of the Privacy and Electronic Communications (EC Directive) Regulations 2003 requires communications providers to keep their networks secure. Responsibility for enforcement currently lies with the Information Commissioner. Are you satisfied the Information Commissioner is best placed to monitor network security?
Margaret Hodge: We have two regulators really operating in this space. We have the Information Commissioner, who has responsibility for personal data, information about the individual, and we have Ofcom, which has responsibility for the regulation of the networks and continuity of supply. I think in that question the interpretation is somehow that the Information Commissioner has got the responsibility around the networks. He has not. Just on the more general point there, Ofcom is just about to put out, I think, a consultation. I think we have done a bit of this today, have we not, about things about to come out, but this is a consultation which is about to emerge on the scene from Ofcom looking at the general conditions around this area and I think security will feature quite prominently, as I understand it, in that consultation, so it may well be that many of the issues raised by this Committee will be taken up in that particular consultation. The only other thing to say, as of course I am sure you are aware, is that Europe has the overarching responsibility here on legislation for communications providers and they, too, will be looking at the issue of security, so we will have a double take on it.

Q875 ***Earl of Erroll:*** I think the real worry is about the Information Commissioner's powers. For instance, when a laptop was recently stolen the Nationwide ended up being fined £980,000 by the FSA, just under a million pounds. It was a huge amount. But when the banks put unshredded statements into the bin, then that comes under the Information Commissioner's office and all it can do is impose a fine of £5,000 if they actually did do it and they were repeat offenders. Online websites are being broken into and details being stolen repeatedly, and in fact I noticed that yesterday or the day before on the Serious Crime Bill which is going through the House at the moment the Minister kept saying that the great protection is the Data Protection Act and the Information Commissioner. Does the Information Commissioner really have the powers and ability to enforce these things properly, because you seem to place a lot of reliance on him but he has very little power?
Margaret Hodge: He has the powers and he could make a recommendation to us around issues such as fine levels. Again, my understanding is that he is considering that at the moment, but when he looks at fine levels in relation to individual data in this area he has to look at other areas where there are abuses of legislation. Let me give you an example. My postbag as a minister around issues which go to the Information Commissioner is much, much larger around TPS, the Telephone Preference Service. I get many more letters from MPs around abuses of that than I do around any abuses in relation to the Internet. In his review of an appropriate fining regime he has to have regard to the rather broader areas of crime and breaches of the legislation than simply looking at breaches relating to the Internet, and it is interesting to see that they are not big here. They do not feature massively in his in-tray. I assume he has given evidence to you already and I do not know whether he said that, but certainly my perception, as a minister, is that he gets more.
Chairman: He said that, yes.

Q876 ***Earl of Erroll:*** It may be because people do not realise and the penalties are inadequate.
Mr Coaker: Could I just say that there has been a review by the DCA of penalties in respect of the misuse of data and I think that is now reported and what the Government is now looking at is a vehicle to actually look at increasing some of the penalties available for the misuse of data and finding an appropriate vehicle to take that forward.

Q877 ***Chairman:*** I think perhaps people can remember a day when the telephone did not have that problem and as they have only recently acquired a computer they think that the problems have come with the computer!
Margaret Hodge: It may well be.
Mr Coaker: The increased penalties for the misuse of data is something which is being taken forward.

Q878 ***Lord O'Neill of Clackmannan:*** A related matter about fines. We have had a lot of complaints about email spam. Does the Government intend to raise the level of fines for spamming and block the loophole of business to business span?
Margaret Hodge: This goes back really to the question we have just discussed. I had forgotten that point about the DCA and it may well be that arising out of that DCA review the level of fines will go up. The only other thing I can say to you which might be of help is that the advice to us from the Information Commissioner is that speed is more important to him. At the moment the investigations just take too long and I think if he would prioritise any issue he would go for speed more than fine levels as giving greater consumer satisfaction.

Q879 ***Lord O'Neill of Clackmannan:*** What about the question of companies, as they do in the States like AOL and Microsoft, bringing anti-spam cases to court? They seem to be under the impression that it is rather more difficult for companies like AOL or Microsoft to bring a legal action of this kind on behalf of third parties in the UK.
Margaret Hodge: I am slightly baffled on that one.
Mr Smith: I am not sure I have got a very strong answer to that. I do not think there are many spammers left working out of the UK, I think they are down to single figures, I suspect. Most of them are in the US, China and Eastern Europe, so whether Microsoft would actually need to take such action in the UK is debatable.
Margaret Hodge: Can we write to you?
Lord O'Neill of Clackmannan: Yes, I was going to suggest that. I am not trying to ask you a trick question, but if you could pause and reflect and then write back, I think it would be helpful. Thank you.

Q880 ***Lord Young of Graffham:*** At different times in my life I have applied for a wire line licence and also a mobile licence and all of them had pretty robust conditions about 999 emergency services. I understand the point that the Association of Voice Over IP Operators wishes to provide those services, but there is no way it can provide the same robust services. Are there plans within either department to begin to vary these conditions to enable them to do the same?
Margaret Hodge: Ofcom on the Government's behalf is currently in discussion and negotiation with the EU Commission to look at those regulations to see whether they cannot be more appropriate to the new methods of communication, so I completely take that point, but I would again make the point that the certainty of access to a line when you have 999, if we are not going to have it with some of the new platforms then we have got to do a lot about consumer information so that they do not rely on it, and we have got to do a lot about ensuring also that providers do the best they can given the limits they have in that they do not control the network.

Q881 ***Lord Howie of Troon:*** There is very little research into computers done in British universities. Only a very small number do it. Do you think that the research base is being adequately funded?
Margaret Hodge: I am told that there are about 30 projects currently in the UK university sector which are funded and are looking at computer security, and I am told that relative to the "asks" this is not a bad take-up. We have got a number of universities, Cambridge is one, which have five stars.

Q882 ***Chairman:*** Our present adviser is one of the staff!
Margaret Hodge: There you are! There are others, a list of six universities, Cambridge, Imperial, Manchester, Southampton, York and Edinburgh who have got a five star rating in the last RAE, so we have a good competence, as with your adviser, in our university base and they are presumably applying and I am told not doing badly. The only other thing I would say is that we have got this Knowledge Transfer Network, which is an important mechanism for the sharing of knowledge and information between academics, and between the academics and the industry, and we are also developing an innovation platform around network security, which I am sure your advisor is also linked into. Those are two mechanisms where we have been successful, really developments within the DTI, to look at cutting research areas, of which this is one. So I am told there is not a problem, which is why I was quite surprised to see your interest in this. You will never get all the money you want, the world being what it is, but I am told that we are not doing badly in this area.

Q883 ***Chairman:*** It is a subject of broad social interest, is it not, so a personal observation of mine is that perhaps there could be more research—and there is research in Oxford and places—on the sociological aspects of some of these issues.

Margaret Hodge: Yes.
Mr Smith: Could I just add, that is the reason we established the network and information security platform to take this kind of horizontal view of the problem, and the platform idea is to actually take these big issues and then try and bring in a kind of multi-disciplinary approach to research in this area. We can certainly provide more details to you on how that platform is working.

Q884 ***Chairman:*** We did visit CITRIS, just such an institute at Berkeley in California, and that was quite a large team of people with tentacles all over the country, which was quite impressive.
Margaret Hodge: Funded by?
Chairman: It is funded by NSF partly. I think it is largely NSF and from industry.

Q885 ***Lord Howie of Troon:*** It is a partnership between the academics and industry.
Margaret Hodge: Clearly, the more we can do, the better. We always like to be at the cutting edge.

Q886 ***Lord Harris of Haringey:*** When is the Crown Prosecution Service going to produce guidelines which will reassure those witnesses who have talked to us, who specialise in IT security and whose work is in danger of being criminalised by the Computer Misuse Act?
Mr Coaker: We expect that to be by the end of the summer.

Q887 ***Lord Harris of Haringey:*** "Summer" defined as being –
Margaret Hodge: A civil service summer!

Q888 ***Lord Harris of Haringey:*** You mean sort of November, yes! Early summer?
Mr Coaker: The end of the summer. If I said early summer, Chairman, I think I would not be as frank with the Committee as I could be. End of the summer is the best estimate. We know this is an important issue for industry and we know that they are expecting the guidance to clarify the position with respect to the new Schedule 3A offence. So it is an important issue and we are aware of the need to ensure that that is done as soon as possible. As I say, without trying to be unhelpful to the Committee, we are looking at the end of the summer for that.

Q889 ***Lord Howie of Troon:*** Could you add the year?
Mr Coaker: This year! I can say, Lord Howie, if you want certainty in our answer, this year!

Q890 ***Earl of Erroll:*** So what is industry doing in the meantime, crossing their fingers and praying?
Mr Coaker: We are consulting with them. We are trying to ensure that the industry's views are taken on board and we are discussing that with the DPP so that we have the appropriate guidance which will give industry the reassurance it needs.

Q891 ***Lord Harris of Haringey:*** But has that section come into force?
Mr Coaker: Yes.

Q892 ***Earl of Erroll:*** Just a quick question. Education keeps coming up. Do you think online training and education should be part of the National Curriculum?
Mr Coaker: As you know, ICT is compulsory in the key stages of education and the QCA is looking at ensuring that online safety is part of the ICT study arrangements for key stage 3 from September 2008, so I think that is something which will be of value, but on its own it is not sufficient and it is good to see that in all stages of education, including primary schools, there is increasing emphasis on this. It goes back to Lord Mitchell's point about the importance of education from an early age, not only with parents but with young children, and so on, to teach them that this is a fantastic tool which opens up all sorts of opportunities and educational possibilities, but it is also something, we need to be aware of, which can be misused. There is increasing work going on in school and it will be a requirement from the QCA, as I understand it, in key stage 3 from September 2008 for there to be safety online.

Q893 ***Earl of Erroll:*** One of the problems, of course, is that there is a lot of different websites. You have got Bank Safe Online, Get Safe Online, and I heard a rumour the other day that the Get Safe Online funding is falling back. I do not know whether it is true or not, but it is very difficult to know which website you go to. Different people are recommending different sites. Should there be perhaps a bit more of a joined up approach, because one of the things which is coming out is that with a lot of people, because they find it difficult to find the resource for this, there is a sort of "blame and frame" culture of saying, "Well, it's their fault. The 80 year old should have known how to do it," or, "The 15 year old should have known better than to go online," so should we have a more joined up approach to all this?
Mr Coaker: I think that is a very fair comment to make and actually if we talk about crime or the use of the Internet the technology is advancing at such a

pace that we need to run a bit more to keep up, and I think coordination and looking at what is happening across all of the various bits of government, all of the various bits of industry, is something we need to become smarter at. No doubt in the evidence you have taken, and in the evidence my fellow Minister and I have tried to give we recognise that coordination of the activity and looking to see how we can make that more effective will have to be part of the work we do in the future. I think it is a very fair comment you have made.

Q894 ***Earl of Erroll:*** Yes, and giving a bit of money to the Met's fraud alert site, for instance, to keep it going?

Mr Coaker: All these things will be considered!

Chairman: Thank you, Ministers, very much for your time. It has been a long session and we have had a lot of questions, and as you have just said and as Margaret Hodge said as well, this is changing so rapidly, this field, and we recognise this and it would be impossible to have all the appropriate regulations in place for something where we do not know what it is part of the time. So thank you very much for your time, and thank you, Mr Smith and Mr Webb. It has been very useful for us and if you have anything else which comes to mind which you think will be useful for us—and I think a few items you were going to follow up on—we will be going on with this inquiry for another couple of months and we would appreciate it if you would send them to us. Thank you very much.

Supplementary memorandum by the Department of Trade and Industry

Q 879 *(third party legal actions against spammers)*

Spam is an international problem and the Government does not collect data on e-mail volumes and the nature of e-mail traffic. Available statistics on the problem vary widely but they do show that the volume of spam is increasing. For example, Symantec, a leading security software company, produce a six monthly Internet Threat Report. This is one of the most widely read documents that measures the problem on the basis of the company's large number of sensors on the internet. The latest report, issued in March 2007, estimates that spam made up 59% of all monitored e-mail traffic in the second half of 2006. This is a steady increase over the previous six months and they found that some 30% of this spam related to the financial services industry. The UK is clearly a major target for spammers but the fact that most is generated by parties outside the UK (and indeed from outside the EU) poses a significant problem in terms of enforcement.

This is borne out by research conducted by Spamhaus[1], a UK-based anti-spam initiative. According to their latest figures, the 200 spammers named on the Register of Known Spam Operations (ROKSO) are responsible for 80% of spam. The list consists of predominately US based spammers and there is only one UK citizen who appears on the list.

It was this background that led us to comment in evidence that we thought it unlikely that action would be taken against UK spammers in the Court. At the time of the session on 28 March, we were unaware that Microsoft had in fact brought two actions. One was against Paul McDonald whose business sold e-mail address lists for the purpose of direct marketing without the holders of those addresses having consented to the receipt of direct marketing.[2] Microsoft successfully sought relief under the Privacy and Electronic Communications (EC Directive) Regulations 2003[3] ("the Privacy Regulations"). The court ruled that McDonald had breached regulation 22 of the Privacy Regulations and that Microsoft, a provider of e-mail services, was entitled to protection under that regulation. Microsoft was entitled to compensation under regulation 30 of the Privacy Regulations for damages as a result of the breach of regulation 22 and also to an injunction restraining McDonald from further breaches.

The second case was a claim against a person who used bulk unsolicited e-mail within the Microsoft Network to attract custom to his pornographic website. Microsoft sued him for breach of terms and conditions relating to the use of their Hotmail service. The claim was settled when the defendant undertook not to send any further unsolicited e-mails and to pay compensation to Microsoft. These actions allow us to confirm the proposition of the Committee that third party legal action is another viable approach to addressing the spam problem—at least for organisations with the resources to pursue such actions.

[1] Spamhaus tracks the Internet's Spammers, Spam Gangs and Spam Services, provides dependable real-time anti-spam protection for Internet networks, and works with Law Enforcement to identify and pursue spammers worldwide. See http://www.spamhaus.org/.

[2] Microsoft Corporation v Paul Martin McDonald [2006] EWHC 3410 (Ch), [2006] All ER (D) 153 (Dec).

[3] SI 2003/2426.

We know that this approach is more prevalent in the US but that reflects both the prevalence of spammers resident in the US and the different legal system. In the US the CAN-SPAM legislation clearly enables ISPs to take spammers to court. Awards there are much higher than the UK, for example a recent Nevada based claim resulted in a fine of $11 million as repayment to ISP customers inconvenienced by a spammer. We do, however, understand that fines are rarely collected.

Q 883 *(how the network and information security platform is working)*

The Network Security Innovation Platform (NSIP) is a new way of working for Government aimed at positioning business and Government closer together to generate more innovative solutions to major policy and societal challenges.

As electronic networks increasingly become critical to society, so Network Security is seen as being a major growth area, and one where the UK is well placed to create added value, through the provision of both products and services. The real "challenge" is to bring together key Government Departments, academia and business to identify both where innovation could be used to solve specific problems and the actions needed to bring Government procurement and innovative business solutions closer together.

The most pressing weakness in network security is the interaction between the system and the person using the system. The key aim of the Network Security Innovation Platform is to bring together technological innovation and social sciences to ultimately create systems that are secure, user friendly, trusted and respect individual privacy. The Platform will aim to place UK business at the forefront of expertise in this area and create wealth by allowing business to compete successfully for major global opportunities.

After consultation two Initial themes were chosen to take forward the platform activities; Human Vulnerabilities in Network Security and Balancing Privacy and Consent in Network Security.

The two areas are dealt with below, showing what activities the NSIP is undertaking, with expected deliverables, time scales and associated R&D spend.

Human Vulnerabilities in Network Security—Restricted Commercial

Four successful Autumn 2006 Technology Programme (collaborative R&D) Proposals were selected—details below. The six month feasibility stage projects started in April 2007 and require a total grant of £350k, with follow up funding of up to £4 million available for successful proposals from 2008–10.

- Integrating Security Technology & Organisational Culture for Employee Risk—BAe Systems, Loughborough University, more industrial partners expected to join the full project stage if the feasibility is successful. The project will deliver a novel organisational and human factors focused network security risk assessment package.
- Trust Economics—Hewlett-Packard Ltd, Merrill Lynch, University of Bath, University of Newcastle and University College London; The project will deliver explore, develop and apply a predictive modelling framework within which the effectiveness and value of security policies that regulate the interaction between humans and information systems can be assessed.
- The Analysis of Human Behaviour from Network Communication—Chronicle Solutions, University of Plymouth; The project aims to develop the scientific basis to support a potential technology solution for the analysis of enterprise digital communications in order to identify and act on potential security threats introduced by humans to information and IT services.
- CatalysIS: A tool to improve risk culture and identify human vulnerabilities in Network Security—The National Computing Centre Ltd, University of Manchester; The consortium believes that a catalyst to improve attitudes towards risks both to and from information systems should be created. The deliverable is a software-based tool that provides a network security awareness programme that is tailored to the individual employee.

Balancing Privacy and Consent in Network Security

The Identity and Passport Service (IPS) is the primary challenge holder in the area of "Balancing Privacy and Consent in Network Security—Using innovation to address privacy and consent in Identity Service Provision". The NSIP is working with the Identity & Passport Service (IPS) to develop a work package that will sponsor research and development into how to balance the intrusive nature of identity services and network security with expectations of privacy and consent.

— ID service provision will both create wealth and reduce fraud, by allowing secure verification of identities. The work programme will be geared to creating a new business sector in the emerging privacy enhancing technology area. A functioning but still embryonic ID services sector will emerge by 2010 and the NSIP will increase the likelihood that secure digital identities will be accepted by the public and will create opportunities for UK business.

— The NSIP will bring together Government Departments, large businesses, retail, banking, innovative SME's and academic partners in collaborative partnerships.

— A joint DTI and IPS workshop highlighted specific scenarios where NSIP activity would have best effect. This formed the basis of a scoping study to identify the key areas for the NSIP to target. The IPS funded study, conducted by PA consulting, will be delivered by July 2007 and will include a workshop to clearly define what challenges the programme should address such as;

  — How do you implement informed consent?

  — How do you prevent further dissemination of private information?

  — How do you revoke consent?

— We expect the R&D activity to be launched in Autumn of 2007. The initial activity will be via an "Ideas Factory" Sand Pit in collaboration with EPSRC and ESRC who have committed over £3 million of co-funding.

Supplementary memorandum by the Home Office

Q 843 *(legality of botnet use) Q 848 (frequency of illegal botnet use)*

The following questions were asked by the Committee at the hearing on 28 March. As the questions range across both 843 and 848, they have been combined.

1. If a botnet is installed illegally on UK machines, probably from abroad, for nefarious purposes, is this an offence?
2. Following on from that, what if the perpetrator can't be identified / found?
3. This botnet is hired out to people in the UK. If they use it for illegal purposes—denial of service, hacking or whatever—are they are in turn committing a CMA offence?
4. If they are using the botnet for something annoying but not necessarily illegal, such as spamming, what action could be taken against them?
5. Is the person who hires the machine participating in the original offence of installing it—ie aiding and abetting the original offence by providing a lucrative market for it? Or is there any other incitement offence or other part of CMA that might apply?
6. What is the legal position of someone who pays to have a botnet attack in order to test security?
7. What is the position of people who unwittingly have botnets on their computers?

The answers to these questions are based on legal advice.

1. This is an offence contrary to section 1 of the Computer Misuse Act—unauthorised access. A section 3 offence has also been committed because a botnet causes an unauthorised modification to the contents of the computer. A section 2 offence may also have been committed depending on the "nefarious purposes" it is used for.
2. If a perpetrator cannot be identified / found then no offence exists.
3. If it is used for illegal purposes, this may fall under the CMA offences, and also under a conspiracy offence, incitement, or aiding and abetting, depending on what has occurred. Depending on what the illegal purposes are, it might be possible to charge substantial offences such as copyright offences or offences under the Fraud Act. It is an offence under section 7 of the Fraud Act 2006 to supply an article (which includes any program or data held in electronic form) for use in frauds.

4. It depends on what they are doing, but charges might be possible under section 127 Communications Act 2003. Depending upon the nature of the spam, harassment charges could be considered under:
   - the Protection from Harassment Act 1997, under which a Restraining Order could be given;
   - Section 1 Malicious Communication Act 1998 which created an offence of sending letters which convey indecent or grossly offensive letter or electronic communication or article. Maximum penalty six months imprisonment;
   - Section 16 Offences Against the Person Act 1861 (threats to kill), and possibly sections 39 and 47 or 20. For section 47 and 20 offences you need bodily harm or medical evidence of psychological injury;
   - Section 2 Criminal damage Act 1971 (threats to commit criminal damage);
   - Section 4 Public Order Act 1986 offences—If the messages—e-mails, phone calls etc cause the victim to fear that violence will be used against them then the police can choose to charge the offender with an offence contrary section 4 which is punishable with up to five years imprisonment and also allows the court to make a Restraining Order;
   - Section 4A Public Order Act 1986 no offence if both parties are in dwelling. If the offensive or threatening letter, electronic communication or other article is racialist in nature or motivated by religious hostility then charges could be brought contrary to 32(1)(a) or 32 (1)(b) of the Crime and Disorder Act 1998, In serious cases offenders could face up to seven years imprisonment;
   - Regulation 22 of the Privacy and Electronic Communications (EC Directive) Regulations 2003 which say a person must not transmit, or instigate the transmission of, unsolicited e-mails where the recipient has not consented or has opted-out under regulation 22(3)). These Regulations can be enforced by the Information Commissioner using his powers under the Data Protection Act 1998 as extended by these Regulations (see regulation 31) or by way of third party proceedings (see regulation 30 and the answer from the Department of Trade and Industry to Q.879).
5. This is possible, but if the action could be proved, and depending what the hacker has done, the offence might be prosecuted under a conspiracy charge under Section 1 of the Criminal Law Act 1977, or an incitement charge under common law.
6. So long as a person has used their own network to form the botnet and the attack is against their own property or they have the owner's permission to carry it out against their property then it is not an offence. The problem occurs when the botnet is formed not of an individual's own network but rather infected machines belonging to others. In such a case the person paying for the botnet attack, if aware that it is not the owners network, could be charged with (depending on the facts) offences of incitement, conspiracy or even aiding/abetting a CMA offence.
7. There is no criminal liability, as people in this position are perceived as victims.

TUESDAY 17 APRIL 2007

Present	Broers, L (Chairman)	Patel, L
	Erroll, E	Sharp of Guildford, B
	Harris of Haringey, L	Sutherland of Houndwood, L
	Hilton of Eggardon, B	

Examination of Witnesses

Witnesses: Mr Achim Klabunde and Mr Merijn Schik, Privacy, Trust and Related Areas, Ms Margareta Traung and Ms Zinaida Yudina, Safer Internet Plus, Mr Andrea Servida and Mr Rogier Holla, Network and Information Security, DG Information Society, examined via video-link.

Q895 ***Chairman:*** Good afternoon and thank you all for agreeing to meet with us. We are members of the House of Lords Select Committee for Science and Technology. I am the Chairman of this Committee and we are in the latter stages of an inquiry into personal Internet security. This Committee looks into issues that involve science and technology but which we feel have an impact upon people in general and upon which we think the government can have an influence. So we have been looking into the security issues that people are faced with in using the Internet. We have been talking to a number of agencies here in the UK and we have visited the United States, but we felt it very important that we talk to you about the EU's work in this area so that we can understand how well the UK is coordinated with those efforts and to learn what you are doing. So that, in the way of introduction, is what we are about. I would be happy to answer any questions before we start with our questions. Do you have any questions for us to start with?
Mr Servida: I would suggest that we introduce ourselves from Brussels and Luxembourg so that you will also get an idea of the role and responsibility that we have in the Directorate-General for Information Society and Media.

Q896 ***Chairman:*** That is an excellent idea. Perhaps you would start by introducing yourself?
Mr Servida: My name is Andrea Servida; I am the Deputy Head of the Unit in charge of Network and Information Security policy and Internet governance within the Directorate-General for Information Society and Media. I will unfortunately have to excuse myself because in half an hour I would like to move to another site in Brussels because I will be joining you with Commissioner Reding later at five, so I will have to leave this meeting to reach my Commissioner. So I will give the responsibility or keeping order on Brussels to my colleague to my right.
Mr Holla: My name is Rogier Holla; I also work in the unit for Network and Information Security and I am in particular responsible for relations with the agency ENISA, the European Network and Information Security Agency.
Mr Bisch: My name is Anthony Bisch; I am working in the same unit as Andrea Servida on the question of Network Information and Security.
Ms Gayraud: Hello, I am Valérie Gayraud and I also work with Andrea on Network and Information Security policies.
Mr Klabunde: My name is Achim Klabunde and I am working in the unit in DG for Information Society and Media, which is in charge of the policy development and of the regulatory framework for electronic communications, and I am leading the team that is responsible for privacy, trust and related issues in this respect.
Mr Schik: My name is Merijn Schik; I work in the team that Achim just introduced and also I am responsible for international co-operation on spam and related matters.
Ms Traung: My name is Margareta Traung and I am working with the Safer Internet Programme, which is run from Luxembourg.
Ms Yudina: My name is Zinaida Yudina and I am working at the same unit as Margareta.

Q897 ***Chairman:*** Thank you all very much. Let me open with the first question and ask you who, in your opinion, is responsible for personal Internet security? Would you like to start in Brussels, Mr Servida?
Mr Servida: Yes, thank you very much. To answer your question I would refer to what we put forward as policy strategy in May 2006, our strategy for a secure information society, and there we have looked at the situation of electronic communication and the Internet in particular with respect to how the situation has changed with respect to what had been the last intervention of the Commission in terms of coordinated policy in this domain. This happened indeed in 2001 and in five years we have seen quite a lot of things changing, in particular with respect to the change of fresh scenarios but also the impact of technology development, which has somehow made Internet develop towards a more ubiquitous type of service and infrastructure. In this respect we believe

that the responsibility for personal information security is a shared responsibility that should somehow involve first of all, of course, the users who need to understand what are their duties and also their obligations and their full responsibilities to protect themselves and also to make their security to be an essential component of everybody else's security, everybody else who is connected through the networks to the devices—the computer, the devices that the user is using for his or her own purpose. Also we believe that it is the responsibility of those who are providing the services to the users because of course the users have not only limited capabilities in terms of understanding what the threats are that are out there and how these threats could become real and not only have an impact to them but also how these threats could somehow be exploited through the users themselves and their devices and to have an impact on others who are connected to the same networks. In this respect we have asked the private sector, the service provider to look at the way they can somehow take up the responsibility of, on the one hand, improving the security of their services, including the security of their systems—software and hardware components—but also possibly be available to even more direct awareness campaigns, which should be targeted to the users who are the ultimate customers of the services being provided by those operators. Of course we should also not forget about the responsibility that Member States and the Commission have in ensuring, on the one hand, that there is a regulatory and policy framework in place which is somehow providing certainty with respect to how to pursue these security objectives and protect the users, but also how to motivate the players—therefore, the private sector operators but also the users themselves—to adopt the technologies and the solutions that already exist and that we hope will be refined through more research and development activities to make the Internet a safe place for everybody to work and to act.

Chairman: Thank you. Would any other of you like to comment on this question? If not, we will go on to the second question and I am going to turn Lord Sutherland, who is three to my right, to ask the second question.

Q898 ***Lord Sutherland of Houndwood:*** Thank you very much, Chairman. Being from Scotland I tend to be interested in money and I wanted to ask a question about the economic impact of Internet-related crime, direct or indirect costs. Can you help give any estimate of what the impact is, what the costs are for the European economy?

Mr Servida: Perhaps I can help in this respect with clarifying something? We at the Directorate-General for Information Society and Media look at the issue of security and resilience of networks from what we call in Brussels the first pillar perspective, which is, I would say, in the light of what is in need of the internal market, the protection of consumers and the other associated aspects which make our intervention needed as well as of the impact to society. For what concerns cyber crime and everything that has to do with more directly third pillar issues the responsibility is more in the hands of our colleagues in D-G Justice, Freedom and Security, who respond to Commissioner Frattini who I understand you are possibly going to contact later on. So in order not to give numbers that might be considered already obsolete by the police I would ask you to perhaps redirect this question to my colleagues who have more up to date numbers than ourselves, in particular because they have a much tighter co-operation with the police service and law enforcement agencies in Member States, which, altogether, I would say, co-operate in defining what is indeed the impact and the size of cyber crime in Europe. Of course, I must also say that while working on the communication that I mentioned earlier, which was adopted in May last year, we have also tried to look at what is the size of crime-related or security-related problems in Europe and unfortunately we have seen that apart from what is in the area of cyber crime we very much lack data that is consistent all across the different European Member States, and in this respect we have indeed requested inter-communication, we have requested ENISA to work with Member States to define a trusted partnership with a view to developing a framework which should allow the collection and the definition of data associated to security incidents and security problems.

Q899 ***Lord Sutherland of Houndwood:*** Thank you very much indeed; we will take this up with the Commissioner.

Mr Servida: There is a colleague who would like to add something, if possible.

Mr Klabunde: I would just like to underline what my colleague has just said. One problem is, of course, that if you say 'cyber crime' or 'Internet-related crime', there is no common definition for these terms, so even when there are statistics produced, the different definitions used make it very difficult to add up the figures and to get a global number. The Commission made a statement in its communication on spam last year where it quoted industry figures which estimated the cost of spam, which is of course not necessarily always crime but often connected to crime, to an amount of 39 billion for the year 2005 worldwide and figures between 3.5 billion and 1.4 billion for the biggest Member States of the EU. But that would only be blowing the snow from the top of the iceberg—it certainly does not give the entire picture.

Q900 ***Chairman:*** It would be helpful if you could say who is speaking as the picture we have of you in Brussels is a little confusing as to which of you is speaking, and it would be very useful for our transcript. So who was that who made that useful comment?
Mr Klabunde: I am Achim Klabunde.

Q901 ***Lord Sutherland of Houndwood:*** I appreciate that lack of data and definitional problems mean that some of these questions will have to wait and we will certainly take the first one up with the Commissioner, but I wonder if you have any sense at all of whether or not countries that have a fairly high broadband penetration are affected disproportionately in any way? The UK, for example, has a comparatively high broadband penetration. Does this make it more susceptible to economic loss in this area, do you know?
Mr Servida: I do not have data so precise as you are requesting. On the other hand, we have been looking at analyses which of course make the connection between what is the potential and the risk of attacks with respect to the deployment of broadband and deployment of advanced technologies because where you have much better or more efficient connectivity it is also working for those who have malicious intentions in the sense that they have more opportunities and a much easier time to attack users who are connected. So the analysis is to some extent an analysis more by implication than by statistics, and we want to do this in order not just to have the data but indeed to follow up what is the effectiveness of policy-making, I suppose at a European level. Firstly I think it would also be good—to have this shared with Member States—is to develop and try to come up with a set of indicators that could be somehow shared by all of the Member States so that in Europe we can have a sense of what are the types of problems and how the policy intervention, the review of the intervention, the technological developments, the adoption of perspectives are indeed changing the features that we would be able to characterise via these indicators. Of course, what we would like to do is to develop such indicators in close connection with Member States because we know that there are a number of Member States who have already developed these types of indicators, these measures, these statistics, and we think we need to learn from those who have already made an effort in this respect in order to possibly spread the best practice that is there in order to come up with direct data for Europe as such and for the Member States in Europe, instead of having to struggle somehow on how to extrapolate from data, which has been developed either for the world as such or from just a region in the world, what might be the type of scenario that we have in Europe.

Chairman: I will turn now to Lady Sharp, who is on my left, to ask the next question, please.

Q902 ***Baroness Sharp of Guildford:*** Could I start by asking you what are the legal bases for EU action and how far do you see Europe's role in driving forward the standards for Internet security? Can Europe move fast enough to keep pace with the changing threats?
Mr Klabunde: As far as the legal basis is concerned I can answer that in so far as the regulatory framework for telecommunications is concerned, which is also the point that was mentioned during the preparation. Here, of course, the main concern for all regulatory actions, not only for those related to security, is the harmonisation of the internal market of the EU, which is based on Article 95 of the Treaty. As far as security- related provisions in the framework are concerned, of course it is quite important for operators which work on a Europe-wide scale to have similar market conditions in whatever Member States and not having to comply with 27 different regimes. So there is an interest of harmonisation. Of course there are other domains on which, due to my responsibility, I would rather not comment in detail. I just mention that in the Treaty on the European Union, as opposed to the Treaty on the European Communities, we have the activities of the Judicial and Police Corporation, which also enable the Commission to support initiatives, but as my colleague, Andrea Servida, has already pointed out, this is not in the main competence of the DG Information Society but in the main competence of Vice President Frattini and of the DG for Justice, Freedom and Security.
Mr Servida: If I may just complete what Achim just said? Indeed, Article 95 is the legal base that we are using for any review for intervention. I must say that what we have adopted as a strategy for Network Information Security is indeed a mix of review of the activities which are addressed to specific issues or problems that we see emerging or that we see as extremely critical, or that we are addressing in view of the ongoing activity on the review of the regulatory framework for electronic communication. Then we have a lot of what we think needs to be done boils down to, I would say, a partnership where we believe there is a lot to be gained by co-operation between public bodies and the private sector. In particular because we see that the complexity of the scenarios and the threat in the private sector is somehow the main player, together with the user, of course, in the Internet, which makes the private sector an important player to act and to be somehow stimulated to act to improve the level of security of the Internet and Information Society. To come to the second part of your question on the standards, I would like to say that to some extent to facilitate and support even more of these public/private partnerships we established in

2004 the European Network and Information Security Agency, ENISA, which is based in Crete, whose legal base is Article 95, and one of the tasks that ENISA is to carry out is indeed the one of following and stimulating the discussion and the co-operation of the private sector with Member States in the area of standards. Of course, standardisation is a changed scheme, if I may so, in particular in these areas over the last 20 years and in particular because the technical developments are so fast that indeed we have assisted with the development of more and more *de facto* standards. I think that Europe has to play a role there and we are motivating, I would say, the private sector and our European standardisation body to play a more proactive role in the area of network information security, and in this respect I would remind you of the Network Information Society Steering Group, which is an activity jointly managed by CEN and ETSI, which has recently adopted a survey of what are the network information security standards that are critical and important for the development of our Information Society. This report is available from the ETSI website and it contains also a number of recommendations for what is to be the way forward and how to improve the standards in those areas that indeed deserve further improvement.

Q903 ***Baroness Sharp of Guildford:*** Thank you very much. Can I add a rider to the replies that you have given me? Under Article 95 presumably you are, as you have indicated, taking forward issues of consumer protection and the single market, but you were indicating that under the justice pillar of the EU Treaty there were very limited powers that you have. But what powers does the Commission have to promote, say, co-operation in policing or mutual legal assistance? Do they have any powers here?
Mr Klabunde: I am sorry if I have not expressed myself clearly enough. When I said it was outside my competence in speaking for the DG Information Society for Media, this is not our competence; but the Commission's DG Justice, Freedom and Security has of course a stronger mandate in this direction to facilitate co-operation of police and in the judicial domain. But that is not in the responsibility of the persons who are sitting at this table today, which is why we would prefer not to comment in detail on these matters.
Mr Servida: If I may just complete the picture because there are also colleagues in Luxembourg who have regular contact with my work colleagues in the DG JLS. In the area of cyber crime our police are working on communications and we have been coordinating our activities, the activities for our strategy of communication of last May, and what indeed they are doing themselves in the area of the coordination of the investigation system and the enforcement agencies and improving efficiency of the judicial system, and we have coordinated our work together in order to aim at the same direction although using instruments that are completely different. In this respect I do not know if our colleagues in Luxembourg would like to say something in this respect? Our colleagues are dealing with the programme on safer use of the Internet and they are actually looking at aspects like child pornography and fighting illegal content and that, in terms of the judicial system and activities, is being handed by the JLS. But in terms of technological and project type of development, these are indeed promoted by my colleagues in Luxembourg and I do not know whether they would like to say something in this respect?

Q904 ***Chairman:*** Would you like to add something from Luxembourg?
Ms Traung: Yes. As far as the Safer programme is concerned for the time being we do not have a lot of co-operation going on with DG JLS but in the future we will try to enhance the co-operation and have closer contacts.
Mr Klabunde: I would make an additional remark, if you would allow me? As I said, I would not want to comment in detail on the interpretation of the legal basis in this respect, but on the ground there is ample co-operation between DG Information Society and D-G JLS on these matters—on cyber crime, on identity theft, on different actions against malicious activities on the Web. So I would just avoid the impression that is created that there is no connection. We are mainly working on the legal basis that we have commented on here, while the third pillar activities are not in the focus of our responsibility and that is why we would not want to make any statements on behalf of colleagues who are not present today.
Chairman: Thank you. I will turn now to Lady Hilton for the next question.

Q905 ***Baroness Hilton of Eggardon:*** Good afternoon. You were talking about the need to stimulate organisations to improve personal Internet security. What incentives do you think will be offered to ISPs, banks and so on, and are you doing things to improve incentives between countries, better harmonisation procedures?
Mr Klabunde: This of course relates to the proposals or the considerations that the Commission has put forward in its working document for the review of the electronic communications regulatory framework, where three options were considered in the context of security-related measures in the framework. One consideration is to find a way of making providers responsible to notify security incidents which lead to the disclosure of personal data or to interruptions of service to the competent authorities. Another one was

to update already existing provisions which concern network integrity, to be aligned to the technological development. And the third one of course is to empower the national regulatory authorities to be more detailed in monitoring the providers and their responsibilities with respect to security measures actually taken on the networks, and to give more precise indications on these issues than is possible under the current system. These are measures which in total could have the effect of increasing the economic incentives to invest in security, of course, in line with other non-regulatory aspects like awareness of the general public and everybody about security risks and a better assessment of the situation by users, by citizens and so on. Maybe my colleagues would like to add something? No.

Q906 ***Baroness Hilton of Eggardon:*** Could we turn to the draft Payment Services Directive, which I understand will reduce the level of protection offered to customers who are victims of card fraud? When we visited the United States recently we were told that customers were only liable for the first $50 and beyond that banks were liable for credit card frauds. Do you see the EU moving towards a position like that in the United States, where banks are legally liable for losses due to online fraud?
Mr Klabunde: I am sorry, we are not at the moment prepared to answer this question.
Mr Holla: We are not working on this particular issue. It sounds like something that may be handled by the DG for Internal Market and services maybe in co-operation with DG for Justice, Freedom and Security. I think it is better to direct this question to Commissioner Frattini and DG Justice, Freedom and Security.

Q907 ***Chairman:*** Let me ask the next question. At the moment all sorts of risks are imposed upon the consumers, for instance by means of end-user agreements, that the consumer will sign very often without fully understanding. However, it has been suggested to us that the key players in the industry—that is the software manufacturers, the retailers, the ISPs and so on—should be made liable for the consequences of security breaches, at least in so far as they can be shown to have been negligent. What do you think about this notion?
Mr Klabunde: When the staff working document of the Commission was prepared it was published together with the communication on the proposals for the regulatory framework of electronic communications. The Commission also collected evidence and assessed all available research and studies, including the data provided by Bruce Schneier and Ross Anderson and colleagues, which you heard, as I understand, in the Committee, and this element has been taken into account in their considerations and will be taken further into account in the decision of what the Commission will propose. The measures that are envisaged are to some extent justified by the assessment that there may be means to increase the responsibility of the economic actors that are in a position to increase the efforts to do more to reduce the problem. But the Commission does not rely exclusively on regulatory aspects, it is at the same time working in partnership with these entities to find a way where everybody can really take their share of the liability and the responsibility and step up their efforts to solve the problem or to increase security by the most appropriate measures, and it is not always necessarily a regulatory approach which proves to be the most successful, so that is part of an overarching strategy which also involves partnership and empowerment, as was pointed out earlier by my colleague, Andrea Servida.

Q908 ***Chairman:*** So I would gather from that there is little impetus within the European Commission to generate a liability regime which would have teeth and would be able to place responsibility with the various partners. I am hearing you say that you feel and the Commission feels that this is just a matter of sharing the responsibility around without making anybody legally responsible for carrying a particular responsibility; would that be correct?
Mr Klabunde: You would not expect me to agree to the statement with the words that you used. I would only want to mention that as far as the aspect of consumer protection is concerned and the contractual and licence aspect that you mentioned, our colleagues in the DG for Health and Consumer Protection are looking in the consumer protection acquis while we are speaking, basically, and are also pursuing initiatives to look into these aspects for potential improvement. But I am not, unfortunately, in a position to make any statement of the state of advancement of these proceedings at this moment.
Chairman: Thank you very much. Lord Sutherland, please.

Q909 ***Lord Sutherland of Houndwood:*** Do you have a view about the value of security breach notification laws, such as my colleagues saw operating in over 30 States in the USA? Do you have a view at all about this?
Mr Klabunde: There are statements even from authorities in Europe which say that as long as we do not have a mandatory notification we do not receive notifications, which means that we cannot prove how big the problem is, which means that we do not have resources to go after this problem, which means that we can do nothing about it, which means that nobody will relay information on this to us. So there are

statements which say that there is a vicious circle as long as the problem is not made known—that nobody will start to fight it and as long as there is nobody fighting it, there is no notification about it. So this would suggest that there is an impact of mandatory notifications if they are implemented in the proper way and in the most efficient and most effective way that would help to better assess measures to be taken to counteract the security problems which are behind these breaches.

Q910 ***Lord Sutherland of Houndwood:*** I am fascinated by the circle that you have drawn there but I understand that the Commission has some draft proposals on security breach notification. These, however, are limited to telecom companies only. The question is bound to be: would it not make more sense to apply these to all companies holding personal data in electronic form?
Mr Klabunde: I would not want to enter into this point as it is slightly out of my organisational competence at this moment. What I can say is that we have the impression that it is worthwhile to look at this issue, in particular for the telecoms sector and not to simply ignore it while we are in the process of reviewing the telecom sector regulatory framework.

Q911 ***Lord Sutherland of Houndwood:*** Perhaps this is one that we can take up with the Commissioner but I wondered if you had had as much publicity in other Member States in Europe as we have had about the recent leak of information held by TK Maxx, which has had a big impact on the general public's perception of the problem?
Mr Klabunde: We have seen reports in recent months for several of these cases which hit the Press—not limited to the UK. We even had a case where a telecoms operator was taken to court by a national authority for a case of leak of personal data, and of course there is lots of data from the United States where, as you stated, quite a lot of state level laws exist, but there is no reason to assume that the problem is any smaller in Europe than anywhere else.

Q912 ***Baroness Sharp of Guildford:*** To some extent this brings us to the E-Privacy Directive. This, I gather, requires communication providers to keep their networks secure. Are you satisfied with the enforcement of these provisions? Do national enforcement agencies, such as the Information Commissioner in the UK have sufficient teeth to enforce it properly?
Mr Klabunde: As I have said earlier, one of the measures that are being considered in the context of the review is indeed to strengthen the provisions which are there regarding security in order to give more opportunities to the national regulators to enforce proper implementation of security measures in the network. We are currently in the process of assessing in detail the issue and looking into the matter to be able to more precisely find a way as to how to do this in the actual proposal of the Commission.

Q913 ***Baroness Hilton of Eggardon:*** If we can turn to email spam and its problems. We have heard a lot of complaints about spam. What is being done at EU level to counteract this problem and is there any scope for raising the level of fines or blocking loopholes, such as business-to-business spam? Do you have any plans in this direction?
Mr Schik: The latest action the Commission took in the area of spam was to publish a communication on the fight against spam spyware and malware, which was released last November. We actually took stock of the efforts that have been undertaken so far on Member State level, by industry, but also identified a number of actions that could be taken up because, as part of the communication, we also set out the fact that the problems are increasing, they are not decreasing and, as was stated before, it is becoming more criminal so there is all the more reason to be proactive also on the Member State level. As part of the recommendations we made in this communication is the emphasis that the need to have a number of critical success factors within central government, which was that first of all we had to struggle with the particular government to actually do something about the problem. It was also to have a clear organisational responsibility within the Member State as to which agency is actually responsible for the fight against spam and related threats, and moreover as part of that strategy to have adequate resources being given to that agency to actually take up the fight because it is quite a knowledge-based activity—you need to have the skills and the knowledge to do online investigation and you need to have some staff dedicated to follow up on complaints that you may receive. So these are a number of suggestions we made in this communication. As far as the legal basis for these activities is concerned regarding the ePrivacy Directive, it is already there. So the ePrivacy Directive already provides for—for example, you mentioned the spam business-to-business—Member States are free to either opt in or opt out of business-to-business emails, and we see that in quite a lot of Member States sending spam between companies is not allowed. So it Member States are free to make a decision there, as sending spam to consumers is banned altogether but for business-to-business Member States can decide to either opt in or opt out. As far as fines are concerned, spam is quite a lucrative business so if you want to stop spammers by enforcing the anti-spam law you have to ensure that you have fines that are a deterrent—if that is the proper work—that you have fines which actually

scare people who are considering to spam others. The ePrivacy Directive allows for these fines to be set but of course it is again for Member States to set the height of these fines—it is not something that the Commission prescribes, it is something that is within the discretionary rule of Member States to decide upon. Further initiatives which I might touch upon to give you some ideas, the Commission provides for a network of spam enforcing authorities, the CNSA who meet two or three times a year, to exchange best practice on how to fight spam and to work closely together and to get the type of cross-border enforcement co-operation in place because, as you are no doubt aware, it is a global problem so we need to have good co-operation set up with other countries in order to actively and successfully catch spammers. This organisation is not the only initiative, plus there is also another which is called the 'London Action Plan', which does more or less the same thing as the CNSA but on a global level so, for example, it covers the US, Australia and Asian countries.

Q914 ***Baroness Hilton of Eggardon:*** In the United States action has been taken against spammers by private companies such as AOL and Microsoft. Do you think it should be made much easier in Europe for companies to take similar action?
Mr Klabunde: I refer again to our working paper and the communication on the regulatory framework where one of the elements considered is also to create a better option to take legal action on civil law level against spammers. So that is an element which is under consideration.

Q915 ***Chairman:*** May I ask you a few questions about ENISA? First of all what is ENISA intended to achieve? Is it doing a good job? And why was it located in Crete where there is an exceptionally low level of Internet penetration?
Mr Holla: That is rather a lot to answer in the time span that is allotted for this meeting! First of all, what is ENISA to achieve? It is a last of tasks establishing regulation—I will give you the highlights—to a collection of appropriate information in order to analyse current and emerging risks; to provide European parliaments, Commission, European bodies and competent national bodies with advice and hence going between different actors operating in the field of network and information security, in particular in the private sector and the public sector, and facilitate co-operation between the Commission and the Member States. These are the most important tasks given the agency. Then is the agency doing a good job? First of all, I should say that the agency has only been operational for a relatively short period of time. Although the regulation established the agency in 2004, in practice it took up its duties in September 2005 in Heraklion, so it is only one and a half years that they have been able to work on operational issues. There has been an evaluation report; the Commission has contracted an external consulting company to do an analysis of the first results that became available. We have recently received this report and it will be published this week on the website of the Commission, available to all. The report makes some criticism and gives some advice for things that could be done better but the overall tone is quite positive. The agency originally has been established for a period of five years and the report advises that the mandate of the agency be extended. So is ENISA doing a good job, the short answer would be yes. Why has it been established in Crete? This is a decision of the Council of Ministers and the relevant national government. It is the Council that decides upon locations of agencies and the Council decided to place this agency in Greece and it was subsequently the Greek government that decided that Heraklion would be its seat.
Chairman: Thank you, that is a very precise and useful answer. May I turn to Lord Sutherland for the next question, please?

Q916 ***Lord Sutherland of Houndwood:*** This concerns an issue that we have come across in our investigations and to some extent a side issue, but since there has been reference to Europe in the evidence we have had we thought we would ask if you had views on this. It concerns the inability of Voice over IP companies to provide emergency 999 calls for police, fire, ambulance and so on. Ofcom, the industry regulator here, told us that the European Union rules are partly to blame for this. Is that accurate and, if it is, why?
Mr Klabunde: The accessibility of emergency numbers from the different types of networks is indeed an issue which is one of the elements considered in the electronic communications regulatory framework. The current version of this obligation is imposed on fixed line operators exclusively, as it was considered to be sufficient at the time of the last revision. It is one of the aspects taking into account the increasing importance of mobile networks and of Internet- based networks on how to implement a proper way of accessing emergency numbers in this context. So this is indeed an issue being considered.

Q917 ***Lord Sutherland of Houndwood:*** Thank you very much, that is helpful. Is there any timescale on when a decision might be taken on this?
Mr Klabunde: The Commission has published a timetable for the review which says that the adoption of the proposals by the Commission is foreseen in the summer of 2007.

Q918 ***Chairman:*** May I ask you a fairly general question about the Internet? The Internet is inherently international; do you feel that Europe is working well with the rest of the world on these issues of the Internet, with America, or locally with Eastern Europe and with the Far East? Do you think that good international co-operation has been established?
Mr Holla: This is a difficult one to answer because the Internet is so pervasive and it is not a single, let us say, part of the Commission or even a single Commissioner under whose responsibility contacts take place with the United States, the Far East and other partners on the Internet—this is a vast area. I personally have some experience in the area of cyber crime, which I dealt with a few years ago. There we had extensive contacts in the framework of G8, which prepared recommendations on this issue and in the Council of Europe which adopted a cyber crime convention. So in that area there is a good international contact. I do not think that anyone here around the table is qualified to speak for the other areas with which we have contacts with third countries. So I am not able to give you an all-inclusive answer to this question.
Chairman: Thank you, that is still useful. If I could turn to Lady Sharp.

Q919 ***Baroness Sharp of Guildford:*** Can I come back to the issue of child protection, which we touched on earlier? Could you tell us what action is being taken at EU level to promote safety on line, particularly the safety of children?
Ms Traung: One of the main actions under the Safer Internet programme is to set up a network of awareness raising nodes in the Member States and the purpose of these nodes is to promote safer use of the Internet, particularly by children.
Ms Yudina: This year we have a particular emphasis on fighting sexual abuse images on the Internet, and there are several areas where we want to contribute in this field. For instance, in May there should be a meeting with Russia on fighting child sexual abuse imagines together on an official level. (Loss of sound connection) We also try to promote co-operation between law enforcement agencies and encourage development of technology for the specific use of police for the analysis of child abuse materials. We are also planning to co-operate with the European financial institutions who can be used as a chain of distribution of evidence of the child abuse material, and we would like to put them together to communicate how they can contribute to the fighting of sexual abuse images on the Internet. The Commission is also planning to arrange a round table meeting with handset manufacturers to foster the development of common standards for handsets that can be safer for children. This is what our programme is doing now.

Q920 ***Baroness Sharp of Guildford:*** Can I follow that up? You may know that in the UK the Internet Watch Foundation—
Mr Klabunde: I believe there is a problem with the connection, we cannot hear you.

Q921 ***Baroness Sharp of Guildford:*** I wanted to follow up my question by saying that in the UK the Internet Watch Foundation has been very successful in closing down a number of child abuse sites. Nevertheless, we only learnt today that there has been a very substantial increase in the amount of child pornography being carried through the Internet. You have indicated that there are quite a number of initiatives now to get co-operation going on between Member States. Is there something equivalent to the Internet Watch Foundation being established at a European level?
Ms Traung: Yes, it is. Actually the Internet Watch Foundation is one of the projects funded by the Safer Internet programme—50% of the funding comes from the EU.

Q922 ***Baroness Sharp of Guildford:*** Excellent.
Ms Traung: The Safer Internet programme gives financial support to a network of hotlines and Internet Watch Foundation is one of its members. There are members in around 23 other European countries, and the purpose of these hotlines is to decrease at the number of child abuse images and others illegal content on the Internet. This means that there are actions ongoing in almost all European countries.
Ms Yudina: It is 24 countries.

Q923 ***Baroness Sharp of Guildford:*** That sounds good. Can I put one final question to you—and this really goes back to some of the issues we were talking about right at the very beginning—how far does the European Union see itself as having a role in educating either children or the general public about Internet security?
Ms Yudina: Our programme has four main emphases and one of them is awareness raising among children and parents. Our programme supports the INSAFE awareness network that is working with schools, parents and children to teach them about the risks that can be faced on the Internet.
Chairman: Lord Harris who has joined us would like to ask a question too.

Q924 ***Lord Harris of Haringey:*** It is a very general question which you might all want to answer but it in the areas in which this Committee is interested, in terms of personal Internet security and the questions about safety on line in particular for children and

other vulnerable groups, are there areas where you feel as officials that you are frustrated because you do not have the power of a mandate to take action? If you had the relevant powers of mandate what would those actions be?
Ms Traung: For the Safer Internet programme we have a mandate to do what we want to do and this is mainly to promote awareness raising and to co-fund the network of hotlines , allowing the public to report illegal content they come across on the Internet.
Ms Yudina: The question is what else we could do. Now our programme has launched an online public consultation to find new areas where we can contribute in the sphere of child protection .

Q925 ***Lord Harris of Haringey:*** And in terms of spam and the other issues that the Committee has asked about?
Ms Yudina: Spam is not for our programme.

Q926 ***Lord Harris of Haringey:*** I am talking to the other officials, whether they feel frustrated about the limits to their mandate or to the powers that they have.
Mr Schik: The short answer is no, no frustration but what there is still—and it is also what we address in the communication—that Member States already provide a lot in terms of legal possibilities to fight spam, spyware and malicious software. But on the enforcement side of things the political commitment is not being put through at every instance into practical enforcement activities and that is something we still hope will improve but it is not taking up the speed we might want it to take up.

Q927 ***Lord Harris of Haringey:*** If I could just press you on that, is there a lack of commitment from the UK government or is it from other areas?
Mr Schik: I am not in a position to comment specifically on the UK government, so I will not!

Q928 ***Lord Harris of Haringey:*** Very wise!
Mr Schik: At the same time we identify the level of critical success factors—and I talked about that earlier. Commitment, who is responsible, what type of resources are dedicated to fighting these practices, what type of fines are imposed, how are spammers or other criminal types deterred from taking up these activities. Those are indicators that one should look at when assessing Member State policy. I can give you an example which is also described in the communication. For example if you take the Netherlands, a couple of years ago they had a strong commitment by the government to take up the fight against spam and they dedicated a team of five to engage in this fight and they invested €300,000 in equipment and material to undertake this and it decreased Dutch spam in two years or so by 85%, which is quite a considerable achievement, and that same team is now also working in other areas such as spyware and malware, building on the experience they have gained. So without commenting on other Member States this is an example of how it could work.

Q929 ***Lord Harris of Haringey:*** But the Dutch example you have given, was the 85% reduction in terms of spam emanating from there or was it an 85% reduction in the spam experienced by users in the Netherlands?
Mr Schik: No, it was Dutch spam because they focused on spam being sent from the Netherlands, being facilitated from machines based in the Netherlands.

Q930 ***Lord Harris of Haringey:*** That is helpful.
Mr Schik: Maybe to give you another example, in Finland they also put quite a lot of effort into securing their networks and to try to clamp up the amount of spam being transferred through the Net and they also achieved considerable success in that. The communication also refers to Finland.

Q931 ***Chairman:*** That has brought us to the end of our questions. It has been very useful indeed for us to be able to speak to you and to get your views. We have access of course to the Commission documents on the website but if there is anything else that you feel would be of interest and importance to us in our inquiry we would very much appreciate it if you would send it to us or direct us to where we can find it. Let me thank you all very much for answering our questions; it will be useful and we will make sure you receive a copy of our report when it is published.
Mr Holla: Thank you very much for giving us an opportunity to tell you something about our daily work.

Examination of Witness

Witness: COMMISSIONER VIVIANE REDING, Commissioner for Information Society and Media, European Commission, examined via video-link.

Q932 ***Chairman:*** Commissioner, we are very grateful indeed to you for offering to talk to us about this topic that we are studying and going to be writing a report on, so thank you very much for being available to us. As you will gather, we are the House of Lords Science and Technology Committee and I am the Chairman of the Committee. We are well into this inquiry into personal Internet security and it will be extremely valuable to us to be able to talk to you to get your views, especially the views of the EU on this important issue. Shall we go straight into our questions?
Commissioner Reding: Thank you, Chairman. I think that will be the most efficient way because there is no need for me now to make a speech here. I think you have questions so let us try to go to the heart of the matter if you wish.

Q933 ***Chairman:*** Excellent. Let me start with the very general question that we asked some of your officials earlier and that is who, in your opinion, is responsible for Internet security? Mr Sevida gave us an answer that of course this is a distributed responsibility but we would particularly like to get your view as to how that responsibility might be distributed and then perhaps to go on and talk about how the responsibility is attributed within the EU.
Commissioner Reding: That is a very large question, Chairman. Of course, the Commission is responsible on the basis of Article 95 of the Treaty, which is the internal market responsibility, so when there are breaches of security which hamper the functioning of the internal market, the Commission has a direct responsibility, and it is on the basis of these Article 95 procedures that all the communications or proposals which come out of my house are based. Having said that, our rule is as follows: try only to intervene when the intervention is absolutely necessary, that is, leave it to public/private partnership as much as possible in order to solve the problems and, most of all, recall that there is a very strong industry responsibility which I would like to be much more proactive, by the way, but which I would like to be based on self-regulation. My belief is that we should not come in with European regulation if self-regulation works. It is only when self-regulation does not work that we should come in on this. Now there are of course elements of responsibility which go beyond the internal market problem and there it is Internet security—I am speaking about cybercrime for instance—and I am speaking about the responsibility which I have taken for a safer Internet for kids for protecting our children. When it comes of course to police co-operation that is not my responsibility any more. I just make this point in order to describe how we see our responsibility. Secondly, we have created legislation, a programme, a fund where we help parents' organisations, for instance, and awareness-raising organisations to tell parents and to tell kids about the dangers. At the same time I have been working together with the industry, for instance with the mobile phone operators who have signed a memorandum of understanding last February that they will provide to parents and grandparents the necessary tools so that parents know about the difficulties which can arise from 3G technology, chatrooms and so on and so forth, and also the filters which are available to parents. The third element is of course when it comes to direct crime when there is a risk of paedophilia. Then of course it is no longer the internal market, then it goes directly to the Commissioner. (Video link broken)

Q934 ***Chairman:*** I think we failed in integrity if not security. If you will continue please, Commissioner.
Commissioner Reding: I have finished my answer. In case you did not hear it all, the last sentence I said was about the responsibility of my colleague Commissioner Frattini as concerns internal security aspects and police collaboration.
Chairman: Thank you for that. I am going to turn now to Lord Sutherland to ask you the second question.

Q935 ***Lord Sutherland of Houndwood:*** Commissioner, is it possible to make an estimate of the direct and indirect costs of Internet-related crime and its impact on the European economy?
Commissioner Reding: I cannot give you accurate figures now but we know that the costs are very, very high indeed. With the analysis we have done on awareness we have found that unfortunately that most businesses, and most of all small and medium-sized businesses, are not fully aware of their responsibility in the security chain which then makes the security chain become very weak, and the loss of ability and the loss of income due to this lack of security is very high, so we have started, on the basis of that, awareness-raising initiatives with the chambers of commerce, for instance, with business groups to inform most of all the SMEs about their responsibility to get their security systems right. The Business Software Alliance also organised an information security awareness day on 27 February this year in order to address these information challenges that technology providers are facing. and this is the first of an annual series which is going to be developed from now on. We know that 90 per cent of EU businesses use the Internet and 50 per cent of consumers, roughly, so you can see the threat through the Internet which can hamper the business world.

Q936 ***Lord Sutherland of Houndwood:*** Thank you very much, Commissioner. I wonder if I can ask two very short supplementary questions. One is you indicated that you do not have the figures in question. Are they available outside this series of interviews in any form that your officials could transmit to us separately? That is question one and the second is, is there any indication that countries that have a higher broadband penetration are more vulnerable to the economic impact of such crime?

Commissioner Reding: To answer your first question, it is very difficult and that is why you see me being very hesitant to give you an accurate answer on this. It is very difficult because we get figures from different Member States which are not on the same level, so to put them all together and make an average would be a false answer to your question, and that is the reason why we have asked for ENISA to develop a framework with indicators which all EU Member States agree upon so that we can get these figures, so maybe in time I could answer your question but I hesitate to launch a figure because this will be then questioned everywhere. The second part of your question was on broadband. There again your vulnerability depends both on the sophistication of the users and of the infrastructure. New methods of fraud are emerging all the time. Broadband going mobile will be a supplementary problem. We do not see it as only one; we see it as a whole chain, so we do not see here governments intervening and then the problem being solved. No, everybody in the chain has to know that he is part of the chain, so if you have a weak part in the chain then that will be a problem. Studies have identified that the penetration of broadband facilitates these attacks because you are always on. If you are always on and you utilise broadband for everything your vulnerability grows unless you have taken very sophisticated counter-measures. Globally the harm done by malware (and these are 2005 figures) is estimated as €11 billion and the phishing element is included in that. That is also the reason why you cannot make it a national issue. Europe-wide is the minimum way to defend ourselves but that again is not enough. That is why I brought this to the attention of the World Conference on Internet Governance which took place for the first time in Tunis and then the last time in Athens and in October it will be in Brazil, so I bring it to the attention of the international community because we do have to fight that together.

Lord Sutherland of Houndwood: Thank you.

Chairman: May I turn to Baroness Sharp now please.

Q937 ***Baroness Sharp of Guildford:*** Commissioner, can I say that we take on board what you said at the beginning about the degree to which your responsibilities are based on Article 95 and the internal market and your wish to use your powers as lightly as possible, to intervene only where necessary, but can I nevertheless ask you how far you see the EU having a role of driving up standards and how far, given that you rely very much on Member States to do this, you feel you have the powers to bring Member States into line to do the things that you would like them to do?

Commissioner Reding: Yes, my Lady, you are absolutely right because we cannot fight this in a regional way any more. We have to fight it at a minimum at the European level and for this we need co-ordination of our actions. If in one Member State nothing is done and in another Member State the maximum is done, both will not have done any good because it is only if we are strong together and if we do not have a weak element in the chain that we can be strong enough to fight. That is also why I have taken the initiative in this May 2006 communication on a strategy for a secure information society where I have appealed to all stakeholders to do their part of the work and that is why we had the November 2006 communication on fighting spam where I asked for a strong commitment by central governments to put adequate resources into the enforcement authorities. That is why in the review of the Regulatory Framework for Electronic Communications, which is due to come this summer, we will address security more closely than has been the case so far. We had a public consultation last year and we got for this more than 200 responses from Member States' national regulatory authorities, the industry and interested parties, so we are really going to work on that to make the security aspect in this new piece of legislation very strong. In December 2006, we adopted a proposal for a European programme on critical infrastructure protection. There is a communication and a proposal for a Directive, thus for binding law on the identification and designation of European critical infrastructures, and on the basis of this work we will take the initiative as a Commission in 2008. In addition to this ENISA is supporting public/private partnerships between Member States and the private sector to reinforce the EU work on standards because that is again another question which we have to take on, and of course my colleague Frattini is proposing now a communication on cybercrime which will complement my internal market initiatives from the point of view of internal security law enforcement.

Baroness Sharp of Guildford: Thank you very much. I think that is very helpful.

Q938 ***Chairman:*** Commissioner, may I ask you a general question about working within the EU between, for example, your first pillar on the internal market and the third pillar on justice and freedom. Do you have formal ways of working together on some of these issues?

Commissioner Reding: Yes and no! When I get a communication, for instance a general communication on critical infrastructure protection, I propose this communication or this draft legislation but of course the other Commissioners who are linked to this come in with their proposals, so it is something which I issue but in the end it is a Commission paper which comes out which is binding for the whole Commission. We have an inter-service dialogue which is permanent on these kinds of issues. The difference now between the proposals I can put on the table to the European Parliament and to the Council of Ministers is that those proposals on the basis of Article 95 internal market rules will be decided upon by majority vote whereas Commissioner Frattini's proposals in the third pillar on security issues are by unanimity, which means that it is very, very difficult in this field to arrive at a common position because any Member State can use the veto.

Chairman: That is very useful to us. Lord Harris, can I turn to you for the next question please.

Q939 ***Lord Harris of Haringey:*** The importance of promoting the information society is clearly your responsibility, Commissioner, and clearly for the public to have confidence in the information society they must have confidence in their personal Internet security, and one of the keys to improving that is going to be to get the incentives right so that those who are best placed to tackle poor security are incentivised to do so. Are you satisfied that the Commission is doing enough to improve the alignment of those incentives?

Commissioner Reding: I am never satisfied that the work that we are doing is enough. Most of all, when you have the difficulty of bringing 27 Member States to a common line in order to be efficient and, not only that, if then also you have to rely on the Member States to apply what has been decided at home in a very a very efficient way, we cannot put a policeman behind every minister to see if he or she is doing their homework so that makes not deciding on common action difficult but applying it very difficult, and it makes it even more difficult if we are in the third pillar in the realm of security because there we are depending on unanimity by the Member States and this is very difficult to reach. By the way, in the Constitutional Treaty two very important things are suggested on this issue. The first one is to have a majority vote on third pillar decisions to make the efficiency of our fight against crime better, and the second one is to permit cross-pillar activities, which are not possible under today's Treaty. We try as much as possible to work together but we do not have a legal base to do that, between the internal market and security affairs for instance. Regarding security, in the review of electronic communications, which are the telecom rules if you want, those are five European Directives which are in place already today but which I will review in the summer, and they are introducing an obligation for service providers and for network operators to inform their customers and competent authorities about breaches of security which result in loss or destruction of personal data. There we will also have an element for updating the provisions on the integrity of networks in order to reflect the technological convergence and the growing importance of IPEA mobile networks in modern society and to improve the implementation and the enforcement mechanisms in order to ensure that the national regulators have adequate and necessary powers to implement and enforce the law. I would also like to recall that we have an E-Privacy (?) Directive which gives the possibility of co-ordinated action Europe-wide but there again the grass-roots implementation, if I may say so, is very different according to the different Member States.

Chairman: Could we go to your question, Lord Sutherland, on breach law.

Q940 ***Lord Sutherland of Houndwood:*** Commissioner, the security breach notification laws, for example, apply in over 30 US states and I wondered if you or your colleagues have a view about the value of such security breach notification laws and what the position is within the Commission on that?

Commissioner Reding: That was exactly what I said to your colleague, my Lord, just before. That is what I will propose in the new Regulatory Framework for Electronic Communications. That will be one of the points. We are going also to look at penalties for not implementing appropriate standards in Internet security. You will probably ask when I propose to do this. I propose to do this in the summer. Summer is an extensive time and I cannot tell you yet the exact date but it will be on the table this year and then of course it is a Court decision procedure which means --- (Video link broken) I will repeat my last sentence. You know that the Commission has the right to propose legislation but it is then for the Member States and for the European Parliament as legislator to decide in a co-decision majority vote on this. I would like to add also, because that is also a partial response to what your colleagues have asked, it is not only on legislation and on the public/private partnership that we are working. In our ICT research programme we have just launched a €2 billion call for proposals for collaborative European research and we have a research priority on security. (Video link broken)

Q941 ***Chairman:*** We are back again, Commissioner, sorry about this.

Commissioner Reding: There is better technology available; I have already seen it! What I wanted to say is that we have devoted a part of our European research in ICT to the security questions.

Q942 ***Lord Sutherland of Houndwood:*** Thank you very much. Can I press you just one little bit further. How far are the draft proposals on breach notification limited to telecoms and would it not be more sensible to extend it to all companies that own large data sets?
Commissioner Reding: Yes, the Regulatory Framework is just on telecoms, unfortunately. When I am speaking to you now what I propose in the summer as a reform of the telecoms package is going to be on electronic communications.

Q943 ***Lord Sutherland of Houndwood:*** We understand that but is there any way in which the broader issue could be raised so this might apply to all companies holding personal data in electronic form? There have been some spectacular cases reported in the press recently where legislation of this sort would be important.
Commissioner Reding: You are absolutely right that this would be necessary. I can give you an example of how we are working on RFID, the radio frequency identification tags, where the problem does not yet exist but where we have proactively started to bring together the stakeholders in order to discuss not only the economic benefits of RFID tags but also the possible problems to personal privacy, so to find the solutions at European level on standards and security before RFID becomes a landslide application. If I want to go further than the telecom rules, I will have to go on a stand-alone regulation, as I propose to do for RFID for instance.
Lord Sutherland of Houndwood: Thank you, I think that clarifies the position but perhaps leaves us wanting more action.

Q944 ***Earl of Erroll:*** Sorry I just wanted to add to that. Surely from a personal point of view it is not just a privacy issue, it is the loss of financial information that is really worrying people and it is when the credit card details get lost by large organisations that really causes the financial grief to the ordinary citizen much more than the breach to their privacy through telecoms data being lost?
Commissioner Reding: Yes, we are looking at penalties for not implementing appropriate standards in Internet security. We are working on our Internet security issue and also on the software providers' liability. You know also that the London Action Plan is high in our priorities. I have very much welcomed the fact that the American President has now signed the SAFE WEB Act so that we can also at an international level start to collaborate.

Chairman: We are going to return to Lord Harris now please.

Q945 ***Lord Harris of Haringey:*** I would like to come back to the draft Payment Services Directive, which I appreciate is not your responsibility but where we have received evidence that the effect of this would be to level down the level of protection offered to consumers who fall victim to card fraud by allowing banks essentially to pass on the risks to customers. What is your view as Commissioner with responsibility for the well-being of the information society of this Directive? Do you not feel that it would be better to move towards the position of the United States where the banks are legally liable for losses due to on-line fraud?
Commissioner Reding: Payment services do not fall under my direct responsibility. That is the responsibility of my colleague McCreevy, the Commissioner for the Internal Market, and here what is concerned is mostly very small payments, so I am not now in a position to give you a very precise answer to your question. I have not studied this question in depth.
Lord Harris of Haringey: I appreciate that and thank you for your frankness, Commissioner, but under those circumstances, given that we are being told that the impact of this would be unfortunate in terms of the transfer of the risk and the impact that this could have on the health of the information society, may we ask that you look at this further and perhaps come back to us? (Video link broken)
Chairman: We are back again.

Q946 ***Lord Harris of Haringey:*** I do not know whether you heard but my final point was that given that we are told that this draft Directive could have a negative effect on people's confidence because of the way in which risk will be transferred, perhaps you can give us your assurance that you will look at this further, and if you are able to come back to us with your views that would be helpful, even though it is the direct responsibility of your colleague?
Commissioner Reding: I am certainly going to speak about this with Charlie McCreevy and have a look at this also with Kuneva, because, as you know, we have a Commissioner especially for consumer protection, so I think together with her we should have a look at what you have just said I am just aware that we go there for the micro payments but not for the bigger payments and I will have to have a look, together with my two colleague Commissioners, at the effect of such legislation and also have a look at where this legislation is in the pipeline for the moment.
Lord Harris of Haringey: Thank you very much.

Q947 ***Chairman:*** Let me ask a question about where we feel responsibility should be placed. At the moment the majority of the risk in using the Internet is really dumped on the consumers, for instance by means of end user licence agreements that people will sign without really understanding them. However, it has been suggested to us that the key players in the industry—software manufacturers, retailers, ISPs and so on—should be made liable for the consequences of security breaches, at least insofar as they can be shown to be negligent. The answers that your officials gave us suggested that you might be considering trying to place some responsibility upon some of these players. Could we get your views on this please?

Commissioner Reding: I have already informed you about the information security awareness day and we do have the debate on the software providers' liability, and here I have invited the private sector, in partnership with the public sector, to be more proactive than it has been in the past. Among other things, the private sector should promote the use and the development of standardised processes that would meet commonly agreed security standards to provide adequate and auditable levels of security and support and an appropriate definition of responsibility. We will follow the development of the industry-led initiatives in this area and we plan to organise a business event to stimulate the industry commitment to adopt effective approaches to implement a culture of security in industry. My Lords, the way we normally proceed is as follows: we do not like to come in immediately top down with heavy regulation. If industry, if the market can sort out the problem we leave the market to do that, but we also say to the market or to the industry, "We do not want this to happen for a very long period of time, so if you can sort it out, do it, and if after one or two years you have not managed to sort it out then we will have to come in with regulation," because here we believe that self-regulation is the best way out, if it is possible. If not, then we have to go to a binding regulation which is potentially costly to the industry.

Chairman: Thank you, Commissioner. Lady Sharp?

Q948 ***Baroness Sharp of Guildford:*** Commissioner, you have spoken in relation to the new Regulatory Framework that you are going to be introducing this summer about the need to improve enforcement mechanisms. I would like to ask you, if I might, about the E-Privacy Directive which requires communication providers to keep their own networks secure. Are you satisfied with the enforcement of these provisions? Do you think that the national enforcement bodies such as the Information Commissioner in the UK have sufficient teeth?

Commissioner Reding: No, we are not 100 per cent satisfied with the level of implementation. We think that you have to improve the implementation, and, as I said before, it is not only deciding on the piece of legislation, it is the enforcement mechanisms in order to ensure that the regulators have adequate and flexible powers to implement and enforce the law because in all these cases I am working together with the national regulators. They are responsible for enforcing the European Regulation and I think, for instance, that there should be the possibility for ISPs to protect the interests of their customers by taking direct action against spammers. That is one of the cases. Concerning the national regulators, not in all Member States do the national regulators have enough powers. You have Ofcom in the United Kingdom which is a well-functioning, serious body, but I tell you that I have a lot of cases in front of the European Court of Justice because of very inconsistent application of European law by the different national regulators. One of my proposals in this new piece of legislation is that I would like to impose an obligation on the Member States to have real independent regulatory bodies. When I say independent, I mean from business, from industry and from government, so that is the basis of the fair implementation of regulation in its full consistency.

Baroness Sharp of Guildford: Thank you very much.

Q949 ***Lord Harris of Haringey:*** You told us earlier that you had been pressing for more resources to be put into enforcement of action against spammers. Do you think that there is more that could be done at EU level in terms of counteracting spam? In particular, would you like to see a raising of the level of fines for spamming and a blocking of loopholes such as business-to-business spam?

Commissioner Reding: Spam is a real problem; we know that. We know also that we have to solve this problem at a world level. We know the countries where most of the spam is coming from and I have started discussions with my American counterparts and I have started discussions with my Russian counterparts on this because one strategy is to have anti-spam action inside Europe and another one on the spam coming into Europe in a massive way. Member States and competent authorities will be called upon to lay down clear lines of responsibility for national agencies which are involved in fighting spam and to have effective co-ordination between competent authorities and involve the market players at national level drawing on their expertise and available information to ensure that adequate resources are made available to enforcement efforts. When I am speaking about international I mean outside of Europe relations, where I speak up very loudly each time I meet my counterparts.

Q950 ***Lord Harris of Haringey:*** In the USA many of the anti-spam cases have been brought to court by private companies such as AOL or Microsoft taking action themselves. Would you like to see it being made easier for this type of legal action taking place in the EU on behalf of third parties?
Commissioner Reding: Well, most of the spam is coming out of the United States, that is for sure. We want companies to ensure that the standard of information for the purchase of software applications is in accordance with data protection laws and for companies to contractually prohibit illegal use of software in advertising and monitor how advertisements reach consumers and follow up malpractice and email service providers to provide a filtering policy which ensures compliance with the recommendation and guidance on email filtering, so there is a very strong responsibility on the private sector. By the way, I am in a relationship with all the providers in security applications, with those from the United States but also those from Europe.

Q951 ***Lord Harris of Haringey:*** Can I change the subject again perhaps to another area where this is outside your direct responsibility which is the question of the policing of Internet security. I appreciate that there are other Commissioners with a direct responsibility but do you as Commissioner for Information and Society see there being a case for establishing a European cyber police force?
Commissioner Reding: I know from very intensive discussions with my colleague responsible for internal security and from discussions with the ministers of the interior for many Member States and with those responsible for Europol and Interpol, that police forces indeed have already established, even if it is not in law, but they are already pursuing those goals and they have very strong international co-operation. I had to look to them for the protection of children, so I was working together with them and I know how they work. At this moment this question you have asked has become a hot topic in Germany. I believe that one has to have equilibrium between protecting our society against crime and thus giving the law enforcement authorities the possibility to utilise (as those who commit crime do) the new technologies but at the same tine we have to pay attention to privacy and data protection. To have this in equilibrium is not an easy task.

Q952 ***Lord Harris of Haringey:*** Okay. Some of the evidence we have received has said that a lot of the organised criminal activity on line is emerging from Eastern Europe. Do you see there being a problem in so far as some of the newly joined Member States—Rumania, Bulgaria and so on—are concerned and do you think there is more that should be done to provide support to the authorities in those countries to deal with the problem?
Commissioner Reding: That is exactly what Europe is for and if you see where the countries which have joined the European Union shortly were some years ago and where they are now, the difference is extraordinarily strong. We help those countries to build up law enforcement and to build up also an independent judiciary system, which is the basis of all democratic development, and the fact that they are members of the Union, they are members of a big family makes the progress here much quicker than if they were outside. We have of course a problem with those countries which are now the new neighbours and on which we do not have the same means of influence. There we can only exercise the necessary pressure in our international relations so that they understand that we understand that they are a problem in security issues. ENISA is also helping with respect to those activities to set up a computer emergency response team and to promote best practice on network security.
Lord Harris of Haringey: Thank you, Commissioner.

Q953 ***Baroness Sharp of Guildford:*** Commissioner, you spoke at the beginning of our discussions about the importance of being able to protect children from paedophilia and of the awareness-raising programmes that you are promoting amongst both parents and children themselves. Can I ask you whether you are taking any further action? For example, in the UK the Internet Watch Foundation has been very successful in closing down child abuse sites. Is anything analogous being proposed within the European framework?
Commissioner Reding: Yes. We have the Safer Internet Programme which is very efficient in helping private organisations, which are the ones who fight against criminality against children. In 2007 this has been supporting the international actions which have been targeted at combating the distribution of child sexual abuse images by developing a network of international hotlines—and I just read now the 116000 telephone number for abducted children—to have a Europe-wide linked telephone number so that we can find abducted children more quickly. We are promoting co-operation between law enforcement agencies. We have helped in our research the development of technological tools for the specific needs of the police to analyse more quickly and more efficiently child abuse materials and we have been engaging with the European financial institutions so that they collaborate in a chain of distribution of evidence of child abuse. Our Keep Safe awareness network now has notes in 24 countries in Europe. We have also this year started public consultations in order to find appropriate ways all together in a shared responsibility between public and partner

institutions. We will follow up with four workshops on this and I think I already told you about the memorandum of understanding by the mobile phone operators which has been signed on 6 February this year. I will have a look on 6 February next year at what has happened there. If the operators manage to set up the necessary security measures for the parents, I do not need to come in. If they do not, I will come in. I plan also to arrange the same kind of round table with the handset manufacturers to see if they can in build the security measures that parents and grandparents would like to have. I am also planning this year to promote co-operation with Russia in this sphere. I have already discussed with my Russian counterparts in order to see some action coming up on the on-line distribution of child abuse materials.

Q954 ***Baroness Sharp of Guildford:*** Thank you very much.

Commissioner Reding: So we are very active on this.
Baroness Sharp of Guildford: Good, thank you.

Q955 ***Chairman:*** Commissioner, those are all of our questions. It has been extremely useful to hear your views and your answers. Is there anything else you think we should consider before we close the session?
Commissioner Reding: Well, Chairman just consider that you have an open door here in Brussels and that myself or my collaborators will provide you all the answers which we can to your oral or written questions in the future. Thank you very much for the work that you are doing and I will certainly have a look at your conclusions.

Q956 ***Chairman:*** Thank you, Commissioner. Your answers have been concise and extremely useful to us, so thank you very much indeed.
Commissioner Reding: Thank you, goodbye.

WEDNESDAY 18 APRIL 2007

Present	Broers, L (Chairman)	Mitchell, L
	Erroll, Earl of	Sharp of Guildford, B
	Harris of Haringey, L	Young of Graffham, L
	Hilton of Eggardon, B	

Memorandum by Jonathan Zittrain

1. My name is Jonathan Zittrain. I hold the Chair in Internet Governance and Regulation at Oxford, and much of my work focuses on PC and Internet security.

2. The fundamental engine of digital innovation has been the generativity of both the Internet and the PCs attached to it. By "generativity" I mean the openness of each to third party innovation. Anyone once connected to the Internet can offer any service or functionality without permission from gatekeepers. Similarly, PC architecture allows third parties to introduce new code to users without the PC or operating system maker serving as a gatekeeper. With PCs and Internet together, new code can spread remarkably easily as one user after another simply clicks "install."

3. This crucial benefit is also the basis for threat. Users can run new and unfamiliar code from unknown sources near-instantly, and when they ask to install bad code, their machines and the data they contain can be just as quickly compromised. With the advent of always-on broadband-connected PCs, a compromised machine can become a "zombie," open to further instructions from afar, and able to execute those instructions continuously, usually completely unbeknownst to their owners.

4. In one notable experiment conducted in the fall of 2003, a researcher simply connected a PC to the Internet that simulated running an "open proxy," a condition in which many users' PCs can unintentionally find themselves.[1] Within nine hours the computer had been found by spammers, who began attempting to send mail through it. Sixty-six hours later the computer had recorded an attempted 229,468 distinct messages directed at 3,360,181 would-be recipients.[2] (The researcher's computer pretended to forward on the spam, but in fact threw it away.)

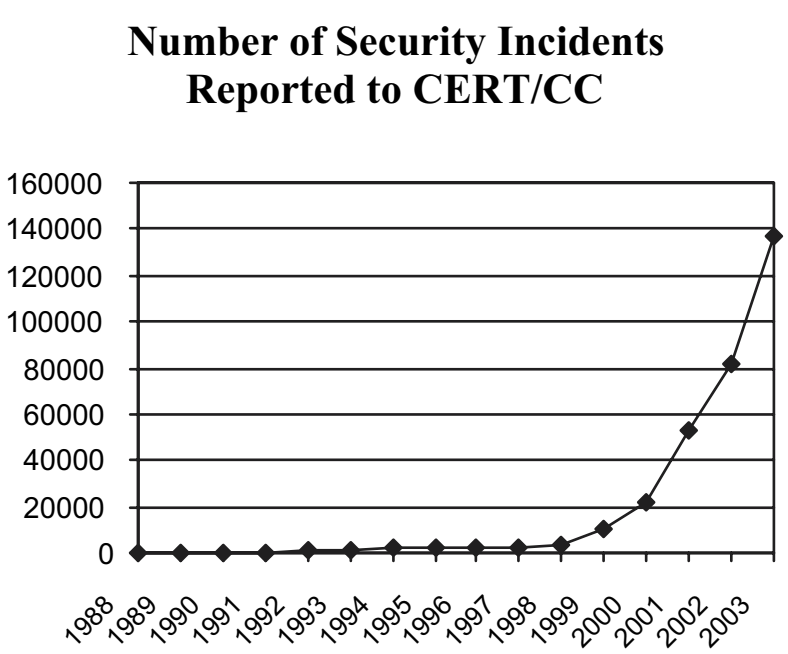
5. The US Computer Emergency Response Team Co-ordination Center statistics reflect a sea change. The organization began documenting the number of attacks against Internet-connected systems—called "incidents"—from its founding in 1988, and they are reproduced below.

6. The increase in incidents since 1997 has been roughly geometric, doubling each year through 2003. CERT/CC announced in 2004 that it would no longer keep track of the figure, since attacks had become so commonplace and widespread as to be indistinguishable from one another.[3]

[1] Luke Dudney, Internet Service Providers: The Little Man's Firewall. A Case Study in ISP Port Blocking (Dec. 9, 2003), available at http://www.securitydocs.com/library/1108 (discussing port blocking, packet blocking, and other methods that Internet service providers could employ to prevent the spread of computer viruses).

[2] Id. at 5.

[3] CERT has also noted the exploding number of incidents of application attacks as a threat as websites increasingly link webpages to company databases. The Risk of Application Attacks Securing Web Applications, SecurityDocs (Jan. 7, 2005), at http://www.securitydocs.com/library/2839.



7. There are several undesirable ways to address the security problem. The transformation from open, generative PC to Internet appliance is one. In the face of a major security breach, or fear of one, consumers will rightfully clamour for the kind of reliability in PCs that they demand of nearly every other appliance, whether a coffeemaker, a television set, a Blackberry, or a mobile phone. This reliability may be offered through a clamp on the ability of code to instantly run on PCs and spread to other computers, a clamp applied either by the network or by the PC itself. The infrastructure is in place to apply such a clamp. Both Apple and Microsoft, recognizing that most PCs these days are Internet-connected, now configure their operating systems to be updated regularly by the companies, often automatically. This stands to turn vendors of operating-system products into service-providing gatekeepers, possessing the potential to regulate what can and cannot run on a PC. So far, consumers have chafed at clamps that would limit their ability to copy digital books, music, and movies; they are likely to look very differently at those clamps when their PCs are crippled by a worm.

8. To be effective, a clamp must assume that nearly all executable code is suspect until the operating system manufacturer or some other trusted authority determines otherwise. This creates, in essence, a need for a license to code, one issued not by governments but by private gatekeepers. Like a driver's license, which identifies and certifies its holder, a license to code could identify and certify software authors. It could be granted to a software author as a general form of certification, or it could be granted for individual software programs.

9. The downside to licensing may not be obvious, but it is enormous. Clamps and licenses managed by self-interested operating-system makers would have a significant impact upon the ability of new applications to be widely disseminated. What might seem like a gated community/offering safety and stability to its residents, and a predictable landlord to complain to when something goes wrong/would actually be a prison, isolating its users and blocking their capacity to try out and adopt new applications. As a result, the true value of these applications would never be fully appreciated, since so few people would be able to use them. Techies using other operating systems would still be able to enjoy generative computing, but the public would no longer be brought along for the ride.

10. An additional incomplete fix is the dual-machine option. Consumers, rightly fearful of security vulnerabilities latent in the generative Internet/PC grid, will demand a future in which locked-down information appliances predominate over generative PCs. One may seek the best of both worlds, however, by creating both generativity and security within a single device. To accomplish this compromise, we might build PCs with physical switches on the keyboard / switching between "red" and "green".[4] A PC switched to red mode would be akin to today's PCs: it would be capable of running any software it encountered. This mode would maximize user choice, allowing participation in unanticipated applications, such as PC-to-PC

[4] For a preliminary sketch of such a division, see Butler Lampson, Accountability and Freedom (2005), available at http://www.ics.uci.edu/cybrtrst/Posters/Lampson.pdf.

telephony, whose value in part depends on uptake by other users. Such a configuration would retain a structural vulnerability to worms and viruses, however. Hence the availability of green mode, by which the computer's processor would be directed to a different OS and different data within the same hardware. In green mode, the computer might run only approved or vetted software / less interesting, but much more reliable. The consumer could then switch between the two modes, attempting to ensure that valuable or sensitive data is created and stored in green mode and leaving red mode for experimentation. A crude division such as this has the benefit of being eminently understandable to the consumer/just as a driver can understand putting a sport utility vehicle into all-wheel drive for off-roading/while retaining much of the leverage and adaptability of today's PC.

11. But such PCs give rise to new problems. For example, ISPs might offer a lower rate for connecting a green PC and a higher rate for a red one/presuming the green to be less burdensome for customer service and less amenable to network abuse. Corporate environments might offer only green PCs and thus limit the audience for available innovation. Or the green PC might be so restrictively conceived that most users would find it unpalatable and would thus continue to choose between traditional PCs and vendor-specific information appliances. Even to hypothesize a green PC is to ask that some way be found to determine which software is suitable for use on an open PC and which is not.

12. We can and should develop new technologies to underpin an open Net. A long term solution doing minimal damage to the generative capacity of the network can be found in two areas of research: development of ways to measure the Internet's overall health and the PCs that are connected to it, and development of programs or methods that allow mainstream users to make informed decisions about how they use the network. A distributed application to facilitate the awareness of large numbers of Internet-connected people about downloadable software and other relevant behavior could have a serious positive impact on the badware problem. An important advantage of such a program over other badware protection software like anti-virus software is that it can take into account the human factors in this security problem, and it can offer protection without creating new centralized gatekeepers that could reduce the overall generativity of networked PCs. Such an initiative would allow members of the general Internet public to trade simple but useful information about the code they encounter. Each would download a simple program that included a digital dashboard to display information such as how many other computers in the world were running a candidate piece of software and whether their users were, on average, more or less satisfied with their computers than those who did not run it. A gauge that showed that a piece of software was nonexistent last week but is now unusually popular might signal to a cautious PC user to wait before running it. Explicit user judgments about code could be augmented with automatically generated demographics, such as how often a PC reboots or generates popup windows. By aggregating across thousands or millions of users, the dashboard can isolate and display the effects of a single piece of code. Users could then make informed individual decisions about what code to run or not run, taking into account their appetite for risk. Its success would depend on uptake, turning users into netizens, citizens of the Net.

13. Such distributed solutions can work beyond badware. They can help us to detect Internet filtering by national governments, paranoid employers, or mercenary ISPs playing with "network neutrality." They can help us to break down rising geographical barriers on the Net, pushing those who still cling to notions like regional windowing of movies and other content to consider business models more in line with abundance rather than scarcity.

14. The information produced by the community can be openly accessible and available to all, the processes of judging applications completely transparent. The database and decision making power need not be with a profit driven company. With a distributed application making people aware of others' decisions about programs and about how they are protecting their computers, it becomes possible to harness the power of the community of Internet users to empower and inform each other so that they can decide for themselves what level of risk they would like to undertake for what sorts of benefits.

15. We need to bring together people of good faith in government, academia, and the private sector for the purpose of shoring up the miraculous information technology grid that is too easy to take for granted and whose seeming self-maintenance has led us into an undue complacence. Such a group's charter would embrace the ethos of amateur innovation while being clear-eyed about the ways in which the research Internet and hobbyist PC of the 1970s and 1980s are straining under the pressures of serving as the world's information backbone.[5]

21 October 2006

[5] For more information on these issues, please refer to: J. Zittrain, "The Generative Internet," Harvard Law Review, vol. 119, May 2006 and J. Zittrain, "Without a Net," Legal Affairs, January/February 2006.

Memorandum by UKERNA

UKERNA[6] is the non-profit company limited by guarantee that operates the JANET computer network connecting UK colleges, universities and research council establishments to each other and to the Internet and inter-connecting regional schools networks.

1. When private individuals connect their computers to the Internet they are entering a public space and are exposed to risks arising out of the nature of that space and the other computers and people who occupy it. As in real-world public spaces the level of risk to which an individual is exposed depends very much on how they behave. In recent years the nature of the most prevalent threats has changed, from technical attacks that target weaknesses in computers and software to "social engineering" attacks that rely on lack of knowledge or careless behaviour by the user to succeed. Viruses, phishing attacks, on-line fraud and trojan horse programs are all examples of the latter type. Software vendors and Internet Service Providers continue to improve protection against technical threats: the greatest opportunity to improve personal Internet safety is therefore to improve users' ability to avoid or resist social engineering attacks that expolit their human nature.

2. While it might be possible, to a limited extent, to impose Internet safety on users, this would inevitably require restrictions on what they can do and, in particular, make developing new services and ideas very much more difficult. Imposing safety (as is done, for example, when we travel by aeroplane) also makes users psychologically dependent on others for their safety and thus highly risk-averse and intolerant of any failure. The statistically illogical reaction of the public to rail and plane accidents, where safety is imposed, contrasts starkly with the response to the much higher, but apparently acceptable, rate of deaths in road accidents where individual drivers feel in control of their own safety. Any approach that attempts to impose safety on users of the Internet is likely to greatly limit the benefits that users, businesses and governments obtain from the network.

3. To achieve the full potential of the Internet as a tool that individuals are prepared to rely on for their daily lives—whether for e-commerce, e-banking, e-government, e-health or many other possibilities—it is therefore necessary to ensure that individuals know how to keep themselves safe on-line. Helping users understand that they can make themselves safer, and providing them with the knowledge and tools to do so, will not only improve their safety practice but also increase their confidence in using the Internet. A recent survey by the British Computer Society[7] found an increase in confidence among home users and attributed this to "a growing recognition of safe surfing and utilising available tools to protect against threats". In a recent paper on social networking for young people,[8] AoC Nilta state that "e-Safety education, not filtering and blocking, will keep young people safe on line". A population that uses the Internet safely, has a stable confidence in it and does not suffer sudden changes of sentiment is essential if plans to provide private and public services over the Internet are to succeed.

4. The stable attitude and consistent behaviour of those users who feel in control may be contrasted with the situation where users rely on others, whether Government or service providers, to keep them safe. Ofcom's media literacy study[9] found large discrepancies between the fears expressed by parents and their actual behaviour: 72% of parents were concerned about their children seeing inappropriate things on line, yet only about half made use of content filtering services. Fear of on-line paedophiles is often expressed, but 40% of eight to eleven year olds use the Internet unsupervised and 23% of twelve to fifteen year old girls mostly use the Internet on their own in their bedrooms. Perception may be very different from actual risk. Concern about on-line "identity theft" is widespread but the BCS survey found only 8% of those surveyed had been a victim; in fact the vast majority of cases are simple credit card fraud which is at least as prevalent in the real world and where the individual's loss is limited by their contract with the issuer.

5. Advice in Internet safety and easy to use tools are already available but these need to be more widely promoted and adopted. For almost all personal computers tools such as automatic software updates, personal firewalls, anti-virus and anti-spyware are available either free or at low cost and can be used without specialist knowledge. Using these tools and checking advice sites such as Get Safe Online[10] and ITSafe[11] should be as

[6] Information about UKERNA is available at http://www.ja.net/
[7] "Britain Surfs Safely" http://www.bcs.org/server.php?show=ConWebDoc.6307
[8] "DOPA, Social Networks and keeping young people safe" http://aocnilta.co.uk/2006/08/03/dopa/
[9] Report on media literacy amongst children http://www.ofcom.org.uk/advice/media—literacy/medlitpub/medlitpubrss/children/
[10] Get Safe Online http://www.getsafeonline.org/
[11] ITsafe http://www.itsafe.gov.uk/

routine as buying cars with safety devices, servicing them regularly and checking the weather forecast before using them. Demand from educated consumers for effective and usable Internet safety will also encourage and enable suppliers to further improve their products, establishing a virtuous spiral of improved safety.

6. Safe use of Information and Communications Technology can be taught, but it should also be demonstrated and applied whenever computers or networks are used. The Qualifications and Curriculum Authority's consultation on Key Skills[12] recognises the importance of these skills as a fundamental part of school education. All members of an information society need to know how to protect themselves and their personal information on-line (whether dealing with e-mail, websites or chatrooms), to assess the reliability of information and communications, to respect the personal and property rights of others and to use and maintain basic safety tools and behaviours. All opportunities to raise awareness, skill and confidence levels of users of all ages need to be taken—children who learn safe practice at school should be encouraged to teach their parents and grandparents at home. Childnet's "Know It All for Parents"[13] is an excellent example of how this can be done.

7. The confidence of Internet users will also be enhanced if they can see that those who misuse the network are held to account. Visible policing of the real world is now recognised as promoting citizens' feelings of safety. Unfortunately the policing of the Internet is much less apparent: the National High-Tech Crime Unit no longer publishes notices of successful prosecutions, regional police forces rarely have the resources to accept and investigate reports of Internet crimes and the Information Commissioner has publicly stated that his enforcement powers are ineffective.

8. Improving all individuals' ability and confidence to use the Internet safely is essential if society is to make effective use of this powerful communications medium. Unsafe users not only put themselves at risk, but are likely to make their computers and networks available for criminals to use to attack others. Addressing these problems requires citizens of all ages to know and practice Internet safety as naturally as road safety, cycling proficiency or motor car care.

Examination of Witnesses

Witnesses: Professor Jonathan Zittrain, Professor of Internet Governance and Regulation, Oxford University, and Mr Andrew Cormack, Chief Regulatory Advisor, UKERNA, examined.

Q957 ***Chairman:*** Welcome, Professor Zittrain and Mr Cormack. Thank you very much for coming to talk to us and to answer our questions and a welcome to those of you from the public and the media who are here. To open, would you like, please, to introduce yourselves and to make any opening statements you might want to make?

Professor Zittrain: Yes. Thank you, Lord Chairman. My name is Jonathan Zittrain. I am the Professor of Internet Governance and Regulation at Oxford University, where I work at the Oxford Internet Institute, and I am co-founder of the Berkman Centre for Internet & Society at Harvard Law School, where I am the Jack N. and Lillian R. Berkman Visiting Professor for Entrepreneurial Legal Studies. I have had an interest in Internet security for at least ten years and my interest has increased in the past four years or so. Many of us are aware that the way the Internet was built was to be able to carry data from one arbitrary point to another without any gate-keeping in the middle. It has been a wonderful feature, so-called end-to-end or network neutrality. This design principle means that any desire to control the flow of data, including data which might be harmful data, is not very easy to effect on today's Internet. There were other networks which the Internet out-competed, so-called proprietary networks, for which, whatever other disadvantages they had, would have had a leg up in battling the kinds of problems the Internet is now facing. There is a parallel problem for Internet end points, things like the general purpose personal computer, which is still the primary device hooked up to the Internet. That PC will run any code you hand it and just as it is great to have a network which will carry any bit from one place to another, it has been the signal event, in my view, of the information revolution that there has been an eco-system primarily comprising general purpose PCs which can run executable code from anywhere. No gate-keeping, including by the vendor of the PC, is in a position to easily stop it. That is because even vendors like Microsoft, who are known to have so-called proprietary operating systems which cannot be changed very easily by third parties, are still putting out so-called generative operating systems where any code can be built by anyone to run on it. However, that benefit, which has so many good implications, is also to my mind the fundamental security problem. Indeed, it is not so much a problem in the network so much as it is in the end points and the problem is not one of Windows versus Linux versus Apple, it is a

[12] Functional Skills Draft Standards: English, Mathematics and ICT http://www.qca.org.uk/downloads/Functional—skills—draft—standards—for—consultation.pdf

[13] Childnet International, Know It All http://www.childnet-int.org/kia/

problem that so long as the user is given the freedom to run arbitrary code from somewhere else then that user can make, and will make, poor choices about what code to run. The implications of a bad choice can be devastating to the user of the computer and it can have spill-over effects to anybody nearby on the network (and nearby on the network need not be nearby in physical space). I believe, Lord Chairman, our central challenge is to figure out how to preserve the best generative aspects of the network and the PC, the ability to run code and data from third parties without undue intervention, while taking on the very real problems which are now starting to flow from exactly that same characteristic. Thank you.

Mr Cormack: My Lord Chairman, my name is Andrew Cormack. My job title is Chief Regulatory Advisor at UKERNA. UKERNA is the company which runs the JANET network, which connects together all universities and colleges in the UK. We also connect schools' regional networks. In the case of the universities, colleges and research centres we also connect them to the Internet. As far as they are concerned, we are the Internet. I started off as head of the Technical Incident Response Team eight years ago, so I spent four years dealing with the consequences of people's bad choices for themselves and for universities. More recently, I have moved to looking at new uses of the network, whether that is new technologies, new user groups, new end points, new devices, IP telephony, the use of telephone converging onto the same network as data—all these sorts of issues—to try and spot any problems, whether they come from people, from technology or from regulatory issues, and to propose solutions, whether those be technological, policy, advice or occasionally regulation.

Q958 ***Chairman:*** Thank you. Let me ask the first question, which we might put in the context of your description of the system and its difficulties, which I think we have a fair understanding of, but given all of that, who should be responsible for personal Internet security and how can they be made to shoulder their responsibility?

Professor Zittrain: A set of short and medium term answers are that everybody needs to pitch in a little bit. I believe that with Internet service providers who find it convenient to maintain the idea of end to end for these purposes and say, "Hey, we just carry the data. It's not up to us whether the digital box we're delivering has a ticking sound coming from it," there are some narrow circumstances in which those Internet service providers can be helpful. At the moment there are some clear tell-tales when, for example, a PC on the network has been compromised, has basically slipped the lead of its owner and is spewing viruses and spam. Interestingly, right now the Internet service provider which hosts that machine will generally not take any action because it creates a customer service event which they then have to deal with, it makes for an upset customer who finds that his network connectivity has been disrupted by the ISP and they do not want to take ownership of it because there is no other economic reason for them to do so. So that is one quick answer. Another answer, which I imagine Mr Cormack will get into as well, is that users themselves can take some responsibility, but they need the tools to be able to responsibly do it, and right now they do not have those tools. There is not even a basic way to know the data which is going into and out of one's machine and without any ability to easily audit it and make sense of it, it is very difficult for the user to say, "Something isn't working so well," and to be able then to take some proactive steps to fix it.

Mr Cormack: I think I would very much agree. I would add that I think people on both sides of ISPs, users certainly, believe that the Internet will become part of normal society. In normal society, individuals are ultimately responsible for their own security and their own safety. I would actually put the problem even earlier in the process than Professor Zittrain does and say that many people—more than 50 per cent according to a recent survey by Get Safe Online—do not even believe that their own behaviour has any effect on their safety. Their safety is somebody else's problem. That is, I think, the most depressing thing I have read for several years because those people are never going to be able to use the Internet as normal, it will always be a special event. They will change into Internet mode where "Everybody else looks after me," from the real world mode where you take care to walk on the pavement outside. I would agree ISPs could do more, some ISPs. On the other hand, ISPs are now starting to advertise the measures they take, which suggests they see them as being differentiators, things that customers will buy. That seems a virtuous spiral where ISPs are advertising security measures, customers are choosing ISPs which offer security measures, therefore they get better.

Q959 ***Chairman:*** You do not see a case for making them legally liable for anything? Bruce Schneier, who talked to us in February, argued persuasively for the imposition of legal liability from a range of parties in fact in the industry, including the software vendors, retailers, ISPs, and so on, and in the event that they failed to use their best efforts to protect customers from security risks then they should be legally liable.

Professor Zittrain: Yes, I am familiar with Bruce Schneier's argument and I disagree with about 80 per cent of it. There is some merit in certain circumstances to establishing a legal framework by which in the most clear cut cases we could see particular parties who but for the flick of a switch

could make something better are asked to do so. To me a great example of that I have already adverted to, which is the Internet service provider who is hosting a machine which is spewing spam and malware, easily detectable, and they are simply neglecting to do it because that is the way the numbers work for them. There might be an opportunity to impose some form of regulation. The rest of Bruce's argument to me adheres to the tricky claim that it is very easy to know what is and what is not a software vulnerability. In the so-called generative systems that I have been talking about, operating systems which are meant to be able to run multiple code from multiple vendors at the same time, it is so easy for one vendor to point a finger at the other and the risk is that should we impose liability on, say, the operating system maker, "Here you go, Microsoft, the animated cursor bug has hit again. You're in trouble," not only would you have some issue as to how to measure and then pay out damages, but you would also have the issue then of Microsoft starting to build so defensively that you would no longer have generative systems. They would start screening their vendors the way that they do for the Xbox video game console. Third parties can code for the Xbox, but they need a special licence from Microsoft before they can sell their software and that greatly constrains the uses to which that box will be put.

Q960 ***Lord Young of Graffham:*** Mr Cormack, you said in your response to the last question, that the Internet should be like normal society where individuals take their own responsibility for their security. But they do not, the police do. Security services do in normal society. It is not up to each of us to look after our security because otherwise that way leads to anarchy, does it not? It does concern me slightly.
Mr Cormack: I certainly would encourage there to be a greater role in policing because I think visible policing actually improves user confidence. I think it was a real shame when the public website of the National Hi-Tech Crime Unit went: it was a very clear public statement of, "We are investigating, we are prosecuting, we are convicting people." I think that was a real blow to public confidence. Certainly in some places the security services, the police, deal with some aspects of security—here, at airports—against major incidents. The things which are causing problems on most of the Internet are not major incidents, they are incidents at the level of losing a credit card number, being knocked over by a car. I do not think we want the security services to be responsible for keeping us safe from those sorts of actions, using a cash machine which has had a device attached to it. At some point the user has to take responsibility.

Q961 ***Earl of Erroll:*** I just want to come back to your ISPs doing something about this traffic which is going through. Will we need to re-write some of the mere conduit defence rules to do that?
Professor Zittrain: I suppose it is possible that there are legal interventions by which we would not want the ISP to say, "I'm just the conduit. I'm just delivering this ticking package. You can't blame me."

Q962 ***Earl of Erroll:*** That is what happens at the moment, is it not?
Professor Zittrain: Right.

Q963 ***Earl of Erroll:*** So we need to re-write our mere conduit rules?
Professor Zittrain: Yes. The reason you find me hesitating, I think, is that "re-write" could be strong. You—at least with the assent of the European Commission—could take a nibble out of the blanket immunity, an immunity which I think has served very well, but say, "Here are some particular circumstances." In many jurisdictions the mere conduit defence, when it rises to the level of actual knowledge of something in progress, can tend to evaporate and the kinds of things I have in mind approach actual knowledge, either in the zombie example I gave or if you are a hosting service for a web server and the web server itself has been compromised—this is now happening with alarming frequency—such that any person visiting the web page in question with a browser which is not properly patched will come away from the website infected; and the person running the website, who may have no technical expertise, who is a merchant who sells products off the site, really cannot be made to care about the problem unless the presence of the malware on that site could have that site shut down.

Q964 ***Earl of Erroll:*** Then why can we not prosecute them under current laws for being a party to fraud?
Professor Zittrain: I think those generally require some level of knowledge.

Q965 ***Earl of Erroll:*** You just explained they do have a level of knowledge.
Professor Zittrain: They might have an alert from somebody which says, like telling the owner of a book store, "I think there's suspicious material on shelf B." They would say, "Well, that doesn't mean I know it, it just means somebody has lodged a complaint and I have to maybe investigate."
Earl of Erroll: That is an offence.

Q966 ***Lord Young of Graffham:*** But telephone companies are not responsible for the conversations which go down the line?

Professor Zittrain: Right.

Q967 ***Lord Young of Graffham:*** They are not even responsible for some of the chat services and other things. Is there not an analogy between the two? How can you make people responsible for what goes on the Internet but they are not responsible for what is on the telephone?
Professor Zittrain: Yes. Lord Chairman, the way I would make the distinction, if there is one to be made, is that in the telephone context the way in which we would imagine the telephone company routinely being in a position to take responsibility for bad things would really require listening in on the phone calls, unless you get into some tricky technology. Here it is not as if we would be asking Internet service providers to greatly change their business model and be significantly more intrusive upon the activities of their customers by having to listen in on everything. Rather it would be, here are some very easily picked up tell-tales, which are almost in an automated way able to be detected, for which the best analogy with the phone company might be, here's a phone which keeps being picked off the hook, keeps calling a particular number and hanging up as soon as the other number answers. The other number complains to the phone company and the phone company says, "Hey, we're just a conduit." On the equities of it, you could see it being less sympathetic to the conduit defence there.
Lord Young of Graffham: Yes.
Chairman: Let us go on investigating your concepts. Lady Hilton, please.

Q968 ***Baroness Hilton of Eggardon:*** I would just like to take up your simile about walking on the pavement. Walking on the pavement is okay if there is a pavement, and secondly you do expect people driving cars not to drive onto the pavement, so I would expect other people to behave responsibly, too. So I am not sure that the analogy totally holds up.
Mr Cormack: I think it is reasonable to rely on responsible other people to behave properly and it is also very useful to have the police come and arrest people who drive on the pavement. I think we are missing that as well to an extent on the Internet.

Q969 ***Baroness Hilton of Eggardon:*** To go back to Professor Zittrain and the "Generative Internet" about which you are so keen, do you not see implications for personal security and safety online if it continues as at present and is developing? There are more and more cases where people are having problems with fraud and phishing, and so on.
Professor Zittrain: I do, and it makes the message of that paper I wrote and the book that I have forthcoming one which upsets people on two sides of the spectrum, to fellow travellers of mine who are technically oriented and who believe that they can solve most of the problems they encounter online, they can program very good email filters, they are smart enough not to be caught by phishing. They tend not to see it as a responsibility of the technical community to intervene to stop the overall phenomenon. I want to argue to those people that they are wrong, that the problems are getting bad enough that if there is not a concerted effort—and it need not necessarily be an effort undertaken through the changing of legal liabilities, and we can talk more about that if you like—to deal with the problem what we will see is a migration of mainstream users and consumers of the network, especially to end points which are non-generative, and I am not keen on that, even as I find those end points very convenient to use, such as mobile phones and Sky Plus and things like that. I want to see the general purpose PC remain in the centre of the ecosystem, including in libraries, offices and cyber cafés where a number of people experience the Internet for so much of a percentage of their lives. If we do not act to fix some of these problems we will see people abandon it, and that is why I am in favour of some form of action.

Q970 ***Baroness Hilton of Eggardon:*** Because with the sort of explosion of use, and so on, it is not at all clear that this can continue, is it?
Professor Zittrain: I think that is right and there may be some elements of it—and this is the 20 per cent with which I agree with Bruce Schneier—which involve some reallocation of legal liabilities, but really the first line of defence will be along the lines which Mr Cormack is speaking of where we need to develop the technical tools so that when people are on the network they can participate on it in the way that we have a radar for each other when we are in a public park. A lot of the security we experience in the real world comes not because the police are just a moment away or there is instant surveillance but because we know that if anything particularly noticeably untoward happens citizens themselves will alert the police, will provide evidence afterwards and may even themselves intervene, and right now there are not good tools on the Internet to allow people to have that same kind of looking out for each other. I believe those tools can be developed. I am part of a project called StopBadware.org jointly among Oxford and Harvard where we are taking some steps to developing those tools and one hopes those experiments will not fail. If they do, they are still learning experiences, but I would like them to work.

Q971 ***Lord Mitchell:*** Is the "generativity" of the Internet a permanent state of affairs, or is it a product of the explosive rate of innovation in the sector over

the last couple of decades, which will then die down as technology matures?

Professor Zittrain: It is certainly a contingent feature. There is nothing inherent about the way the network must always work which will keep it generative, and moreover I think the real nub of your question is, ought we to care about the generativity with the same amount of caring over time, or do we care about it at the beginning when we are sort of trying to subsidise it and then as it reaches its mature uses can we say, "All right, now let's just lock down the secure uses"? Electronic commerce and credit cards may be a good example of thinking about it that way. The way legal liabilities tend to work is that people are not themselves responsible should their credit card be compromised online and as a result they can afford to use something which might scare them or which they do not fully understand, knowing that they have limited liability should their number be stolen and that is seen as a helpful subsidy, at least at the beginning. My view, though, is that while it is awfully hard to predict the future, we are still only in the tenth year of what is probably a fifty year build out of the network and of its uses and there are some tantalisingly promising applications around the corner involving very socially useful and constructive implementations of peer to peer, mesh networks so that we do not need to have major Internet infrastructure, particularly in crowded areas, and data can still get from one point to another, the ability to store data across lots of computers and to have basically a virtual library which does not require one gate-keeping entity to be the Library of Alexandria. These features will not develop if the generative Internet and the end points around it are eclipsed thanks to security fears, so I would at least like to buy us another five or ten years of the generative status quo and then see if it turns out that things have slowed down and we pretty well know the uses to which the network will be put.

Q972 ***Lord Mitchell:*** As part of our investigations we have recently come back from California, from the west coast, and we visited a whole series of companies there. Microsoft and Apple in particular, we noted, seemed to be moving in different directions with Microsoft continuing to facilitate the download of applications but with health warnings and Apple, we discovered on certain products, in particular the iPhone, do not permit any applications at all to be downloaded. I just wondered what you think about that.

Professor Zittrain: I see the iPhone as essentially the poster child, the canonical example, of an utterly non-generative device which is still incredibly useful. Steve Jobs himself last January, in talking about the iPhone, said, "You bet we're not going to let third party code run on it. You do not want to end up with this phone and you run three applications from somewhere and suddenly it will not make calls any more. That is not going to sell and that is the philosophy which goes into the iPod as well." Under very rare circumstances you can re-flash your iPod and try to run third party code on it, but it feels like you are skating on thin ice when you do it and the next time your iPod phones home to Apple to check for updates, if Apple discovers it they might feel themselves entitled to wipe it clean. So I do see that approach from Apple. You see that approach, too, from Microsoft at times, in the Xbox, as I mentioned, in their new Zune. All of these things are not under that old PC model of, "Put out a generic device, call it half finished and let third parties do it." I am not against information appliances, such as the iPhone. I do see them as having a place. I like the idea that you can have the PC as a test bed for an application, you try out Voice-Over-Internet Protocol through something like Skype first and you awkwardly use a headset, and sometimes it works and sometimes it does not, and then some merchant can distil it into a pure appliance size form like Vonage or, say, an iPhone. That is great, but to me that remains great because the PC still is very present in the eco system and should the makers of those tethered appliances, who are always in a position to change the way they operate, get a little too clever, take away too many features, make it, for instance, so that your mobile phone cannot easily clock the total number of minutes used that month, even though many people might find that useful but no third party code exists to do that, you can always fall back to the PC as a safety valve, and without that safety valve I think we would find those information appliances starting to behave very differently.

Q973 ***Chairman:*** What about your concept for a red and green machine? It is a bit like the cell phone. The biggest complaint, particularly, shall we say, elderly people make about the cell phone is that they do not want 90 per cent of it. You could make the same argument for a PC, particularly in certain people's hands. They might want to access information on the Internet, they might want to send email and receive email, but they are not in the game of downloading peculiar programs because they're a geek and they want to try this. I get the feeling—and this might be a bit provocative—that you geeks run this thing and yet you are two per cent of the users, and it might be a good idea to have a green and a red switch.

Professor Zittrain: Yes. Lord Chairman, I brought up the green and the red switch as a way of trying to split the difference because, as you know already, I do not favour the status quo. I see the problem in the status quo and the implication, if no action is taken, that people really will move away from these PCs under just the set of values you mentioned. I see the red and

the green machine, if contained within one machine, as a short-term way to buy a little bit more time, to make it so that within one box you can have some of the reliability and ease of use of an appliance when it is geared into green, but when you or another user of the machine—and so many of these machines are shared machines in a household where the kids are actually eager to go off-roading in a very good way and experiment with new applications, to be able to shift into red but not have accidents from the red machines spill in the green zone. This is seen as a way of trying to split the difference and I would favour those kinds of tools in order to make it happen. It is just that so often tools that start in the province of geeks, written by geeks and for geeks like the Web browser, Mosaic browser, written in the course of a few months, then turn out to be the fundamental building block of the network we see today. If you had tried to sell the idea of a Web browser to CompuServe, America Online and Minitel back in the era of the proprietary networks and make the case for the return on investment for the level needed, how we will market this, all that kind of stuff, at least history the one time we have played it through shows that the browser did not emerge from those circumstances. So to be able to have it come from the geeks, but then maybe it is just one out of a thousand applications which are tried, it can still become so key that it can very easily make that jump into the mainstream because the person who is not a geek has the PC and at some point can double click and run that new application.

Q974 ***Chairman:*** If you know which knobs to disable. I am still frustrated that I cannot adjust the ignition timing in my car when I am driving along. It does not really make a lot of sense to do it, but it was fun when you could do it, but they gave it up rather early because the average person had not got a clue what they did when they changed their ignition timing.

Professor Zittrain: Yes, and I would think that the ignition timing of the car is a good example of what I think Lord Mitchell was getting at with the question about when will we say generativity has worked its magic and we have kind of invented the things there are to invent and now we should lock in those gains and just make it very easy to use and safe. For the automobile, I feel as if over the past 50 years there has not been a whole lot of change in the uses to which we put cars. It is just a question of optimising them under the hood, lowering the emissions, making them cheaper, that kind of thing. With the PC, I do not see us yet in that stage. There are still so many new things which can be done with it that it may well be worth it to take some of the admitted trade-offs which come from keeping a generative system, and the annoyances, and say that they are not the same as retaining a very fine ability to fine tune your car, because by being able to change the ignition timing it is not as if it is suddenly going to fly or be able to take extra people, or do something else radically different from what a car does.

Q975 ***Lord Mitchell:*** If we could move from cars and ignition timing to copy machines and television, you talked about how consumers would rightfully clamour for the same degree of reliability as they get from such products, but it certainly seems to us that you rule out the obvious ways whereby the industry might develop such a relationship. Could you comment on that?

Professor Zittrain: If I understand the question, there is some sense where you just might say, "Leave it to the market." The market will determine through a reflection of consumer preference what the right balance is between generativity and stability, if indeed these things are pitted against each other. I think there is some truth to that, but there are some really important caveats. One caveat is that when people make a purchasing decision the fact is they decide on the basis of current uses, not future ones, and the number of times in the Internet and PC context where we have seen serendipity really pay off, we bought the PC for this purpose but a year later we find we are not using it to keep recipes, we are using it to talk with our kids –

Q976 ***Lord Mitchell:*** It is like text messaging on a mobile phone.

Professor Zittrain: Exactly, and even taking photos on a mobile phone. That is sort of an added feature where you might think, "I never use that thing. I don't need it," but more and more you see such whistles and bells becoming integral and in a purely software environment where it is not a matter of actually having hardware in the machine to get it to perform differently. The cost of trying out those new features in cheap networks is so low—you just double click, you try it out, you like it or you do not like it—and for that reason it is not clear to me that the market will perfectly respond. There is also the fact that those driving the markets have reason, quite naturally—this is market theory at work—to want to have a "winner take all" mentality. At the time you are building an operating system and competing with other operating system makers it is to your advantage, maybe, to welcome as much third party innovation as possible because the more uses there are for Windows created by others, the more copies of Windows there are that will be sold. But the moment you achieve monopoly, then it gets to be to your advantage to try to vertically integrate and see to it that the applications that everybody uses on your now very popular system also come from you.

That is the kind of enclosure which it would be nice if we could have the market naturally resist overall.

Q977 ***Lord Young of Graffham:*** Coming back to your analogy, we are talking about 1920 or 1925 for the evolution of the car. One day, I do not know how long, the software comes along where it is going to be much more difficult for the viruses to infect it, that element of security. You could switch the machine off and switch it on again, but that is another matter. If we intervene at the network level now, presumably the ISP level, we could make users more secure by restricting and denying them the options of taking chances, making long choices. Do people need all the facilities which the Internet provides today, or should we actually go round and restrict people from doing things on the Web?
Mr Cormack: I think I have two answers to that one. The short answer is, I do not think it would help because most of the bad users of the network use extremely simple technology. The email I had from the widow of the late dictator of Nigeria offering me a share of several million dollars was plain text. It was more simple than the email which was sent to get me here, because that had an attachment. The longer answer is, the network has a single function, which is to move packets of information from here to there. Everybody uses that. The model of the Internet very consciously originally was very simple in the middle and all the intelligence was at the edges. You could, in principle, move things to the centre. That would make it more like the telephone network. It would also be challenging to recognise a bad decision. At the moment the network cannot tell, it does not need to know whether something is an email, whether it is a piece of software or whether it is a music download, so whether something is an email I want to respond to or an email I do not want to respond to, a program I want to download or a program I do not, is many, many layers of intelligence above what the network provides at the moment. Again, if you wish to move things to the centre and say, "This is good. This is not," you are assuming you know what will happen in the future. If you had gone to Microsoft ten years ago and said, "Remove the bells and whistles from your operating system," I think the ability to do TCP/IP would have gone very rapidly. It was a passing fad. Five years ago, remove the bells and whistles, there would have been no audio devices, I suspect, so no conversations by IP telephony.

Q978 ***Lord Young of Graffham:*** Of course, if you start doing too much at the centre then you run the risk of becoming a centre, actually restricting what people really do in terms of content, because presumably if you are identifying what it is you can suddenly start to take out words you do not want to appear and things of that sort?
Mr Cormack: Yes.

Q979 ***Lord Young of Graffham:*** Professor, you are on record as arguing that the "end-to-end principle" and the principle of network neutrality no longer reflect adequately the complexities of the Internet. Could you develop this point for us?
Professor Zittrain: Yes, and I appreciate the opportunity to clarify it because to many of my fellow travellers those are fighting words. First, let me make it clear I think the principle of end-to-end neutrality is brilliant. It began as simply a technical heuristic, "Here's a way to build a robust network," and that technical heuristic has proven itself over the years as networks that did not do the end-to-end have not shown themselves as flexible or as powerful, and in that sense I very much like end-to-end. I also am not fond of the idea of content filtering. I co-founded a project now called the Open Net Initiative, which performed the first large-scale enumeration of filtering, common now in over 40 states worldwide. It began with China and Saudi Arabia and extended outwards. So I have got a real commitment against having that kind of filtering take place unnoticed. That said, the kind of modularity that end-to-end suggests—you have the network, keep it open, let the intelligence (as Mr Cormack says) remain at the end points—has a hidden premise in it, and the hidden premise is that the people at the end points can control those end points and make intelligent choices about how they will work. If that is the case, it is just saying, "Let the market work its magic. People will buy the end points or configure the end points as they want." Now that the network is so mainstream, we are grappling with what we have talked about over the course of this hearing so far, which is that people will make poor choices and that often people do not have these end points in their own true custody. That can either be because the computers and other devices they are using are issued by their employers or by libraries, and in that sense they are not a real end point in the technical sense, there is some middle out there that controls it. It is also true in the sense that the so-called tethered appliances we have been talking about, a Sky Plus box or a mobile phone, which can be instantly re-programmed at a distance by its maker but not re-programmed by any third party—and I would put the iPod and the iPhone into that category—these really also push the definition of end point. In my book I have collected a number of examples which remain surprisingly obscure to me of regulators realising the power of the end point and doing such things. In a patent case between EchoStar and TiVo, digital video recorder makers, TiVo won against EchoStar, saying that EchoStar's digital video recorder had infringed the patent. They got money out of a Texas jury, but additionally they got an order from the judge saying that EchoStar must

send a signal to the EchoStar boxes placed with consumers around the world and fry the boxes at a distance. That is a form of remote control occasioned by a regulator which end-to-end does not protect, and that is why I say we need now a more holistic approach. That modularity is helpful for technical reasons between the end point and the middle, but we now need a more holistic approach to understand the regulatory possibilities within the collective network.

Q980 ***Earl of Erroll:*** Can I just ask, did they actually do that, because surely there are in a sense some legal jurisdiction problems and trade implications there?
Professor Zittrain: There are wonderful problems waiting to be taken up –

Q981 ***Earl of Erroll:*** Did they fry the machines?
Professor Zittrain: The order is stayed pending an appeal. The order was issued last August but the case has been on appeal since, so no, nothing has been fried yet. I will say that the basis of the appeal is not on the draconian nature of the remedy, instead it is that the jury got it wrong and the patents are not really infringing, that sort of thing.

Q982 ***Earl of Erroll:*** There must be a major legal problem of jurisdiction if you start frying people's computers which have been sold legally in other jurisdictions? If that happened in Britain, we could sue all sorts of people up the line.
Professor Zittrain: I think that may be so. It can certainly create potential causes of action between the users and the vendor, EchoStar. On the other hand, from a pure jurisdictional point of view, it is possible but not certain that the plaintiffs will say, "You, court, have jurisdiction over this defendant EchoStar and you can order EchoStar on pain of contempt or additional damages to perform any action around the world in order to bring itself in compliance." Now, you might say an EchoStar box installed overseas is not infringing a US patent, but should they find that the patent extends to that, that that caused a sale of a TiVo to be lost, I do not think the issuance of the order alone need occasion a jurisdictional conflict. But it is a good question, I agree.

Q983 ***Earl of Erroll:*** It is, yes. I am going to explore one of the other things a bit further, which is that UKERNA's written evidence argued that imposing safety can make users psychologically dependent on others for their safety and thus highly risk-averse and intolerant of any failure." We see this, for instance, in other people's attitudes to the relative risks of air and train travel versus car travel, but even car travel is actually highly regulated in many ways and in terms of car design, driving standards, road standards, policing, all those sorts of things. A balance needs to be struck, but is the balance that prevails in Internet services the right one?
Mr Cormack: I think it is heading in the right direction. Since writing the submission, I think I have probably modified my view. I think it is now a bicycle rather than a car, but I think the question actually makes the point very nicely that safety in a car depends on multiple factors. It depends on the individual, it depends on the individual being qualified to drive, it depends on the car being checked annually for safety once it gets to three years old and it depends on roads being well built. Some of those the market will deliver, I believe. As I have already said, I think the ISP market is now on a spiral heading towards well-designed networks: at different speeds, but I doubt that anybody's security systems are going to get worse. Whether we want to introduce Internet driving tests or compulsory annual testing at the owner's expense on PCs, I do not know. Having done time on help desks, I would love to be able to say to a user, "You are just too incompetent to use this system. Go away," which is what a driving licence would allow you to do. There is something which I did not mention earlier. There are actually some regulatory pressures against doing the right thing. The mere conduit defence, I think you have mentioned, where in fact the definition of that means that because it is a binary switch you are either a mere conduit or you are not, and you cease to be a mere conduit when you select the information which is delivered. There is at least a concern that an ISP, certainly if it introduced filtering, is selecting the information which is delivered. I do not know about ISPs, but I know colleges have expressed their concern that if they filter, it is actually worse to try to filter and get it slightly wrong than not to try to filter at all. That is actually the law working contrary to what we would like to do, so I think there is a problem there.

Q984 ***Earl of Erroll:*** Just to explore the ISP a bit further—we have actually discussed it, but to make it slightly more specific, we know that the ISPs can detect when attacks are coming from insecure machines and maybe we should require them to do more. Specifically, do you think it would be a good idea to force the ISPs to do more to fix the machines proactively, as we were talking about then, and if we did do that should it really be through incentives or through regulation?
Mr Cormack: I think forcing the ISP to fix the machine feels like a very, very bad idea, if nothing else because there would be a huge liability. As Professor Zittrain has suggested, you have no idea what is on that computer. The user could have downloaded absolutely anything. Your attempt to fix it could well start the whole thing to stop working.

Q985 ***Earl of Erroll:*** Because you could not select a target, the botnet?

Mr Cormack: You could attempt to remove the botnet software. However, the software is likely to have added things at a sufficiently low level in the operating system to conceal its own existence from the user. Removing that could well make the operating system extremely unstable and crash at some later point, and I think the users would then have a reasonable complaint against their ISP. I have some sympathy for the idea that if an ISP sees a large amount of traffic coming from an individual machine it should reduce that machine's ability to harm others, whether by blocking its content entirely or whether by reducing the band width, or whatever. I think those are possible. Whether the solution would scale to the size of large ISPs, I do not know.

Professor Zittrain: To start to get at that question, I want to stick with the traffic analogy for a moment. I have been intrigued by a movement in traffic management called "Unsafe is Safe" and in a number of cities in Europe, including the Dutch city of Drachten, they have implemented something called Verkeersbordvrij—I know I am not pronouncing that properly—which is the absence of road signs, and I actually think there might be a neighbourhood in Kensington where this is being tried as well. It is completely counterintuitive, at least to me, but by removing in the Dutch case nearly every sign and having only two rules (one is to generally be careful and the other is not to park your car in a way that other cars get blocked, but otherwise they have eliminated even parking spaces, you just park the car wherever it is not blocking somebody else) there has been a remarkable decline in traffic accidents. Part of what they attribute that decline to is that it compels people to actually be much more aware of their environment and of other drivers. They have to take responsibility for their own safety, and it means that they do. Whether that would work in every city in the world is highly dubious and trying to transplant that to the Internet context, where it is much harder to make eye contact with other users and when the harm that one can cause is not as symmetric—if you get into a car accident you do not only dent the other car, you dent your own—these are some of the puzzles to cure, but I actually think there do exist cures that we can try and code which represent what you describe as the incentives route before trying the outright regulation route. One example of that would be—I mentioned StopBadware before—we are working with a number of companies, including Google, so that when we see one of these websites which is spewing malware, and we can detect it automatically, we add it to a list. Google shares the list with us. We also make it available to other search engines. When somebody performs a search and one of these sites which has the badware on it comes up as a hit, it does come up but then it has an extra line in the hit provided by Google which says, "Warning, this site may harm your computer." If you click on the link anyway, instead of going to the site it takes you to an interstitial page provided by Google which says, "No, we really mean it. We think there's badware on this site. We recommend that you back up and try another result. If you really want to continue, okay, you may highlight, copy and paste the URL and go on." In our experience partners like Google have found approximately 30,000 sites in the past month which meet these criteria. The webmasters of the sites see an over 90 per cent drop off in traffic when the interstitial is added. At that point the webmaster goes from a level of priority for fixing the site which was achieved by only warning but not having the interstitial, I would say tenth on the list of things to do that day, to it is the number one thing, and I do not care if it is a weekend or a holiday, that webmaster was desperate to get the site back up. It may be an over-incentive, but that is a great example of a collaborative effort run under a .ac or .org rubric in cooperation with dotcom, hopefully spread out enough so we are not creating some new gatekeeper which might then abuse the power to put up the interstitial, which allows us to have people making the eye contact and expressing, "Actually, your car is blocking an entire river of traffic."

Q986 ***Chairman:*** How much of the useful, valuable generative function of a PC would be lost if you only allowed it to communicate on the terms of the user of that PC, if you did not leave the door open completely? You would lose this sort of grid computing potential we hear about, but people could sign up for grid computing if they wanted. If they did not want to sign up their computer to be in a grid, I cannot see why you cannot stop people coming into that computer and using it as a botnet, as a zombie. I just do not understand that and I am not convinced by anybody yet. Perhaps you can convince me. Richard tries all the time, but can you convince me that that is just not possible, so that the PC will communicate when you ask it to communicate? I am told you have absolutely no idea, your computer is sitting there, spewing out Viagra ads to millions of people and you do not even know it. I find that ridiculous. You should be able to provide that capability and tell the person, "This computer is spewing out Viagra ads. Do you want it to do that?" I just do not understand this.

Professor Zittrain: I think each of us is eager to take a crack at it.

Mr Cormack: Two points. The initial software gets there by invitation, almost universally. The initial software is not software, it is an email message saying, "Here is something attractive, something you want. Please download it." So the user is fooled into

inviting the software in. On the question of subsequent transmission, there is plenty of software available already which you can put on your own computer which says, "The following program is trying to communicate with the Internet. Do you wish it to do so?"

Q987 ***Chairman:*** I had that on my machine, I know. Why do not all machines have that? Why is it not compulsory?
Mr Cormack: I would ask high street computer vendors. I would love to see that sort of software on machines routinely.

Q988 ***Chairman:*** It is a bit like turning the engine off. I do that. One of the troubles is that the handshaking time to connect on a lot of things, particularly wireless networks, is tedious. It is like the internal combustion engine, it does not turn off every time you go to the lights because you have got to crank up the electric starter and get it going again, whereas an electric car can do that. I do not see why we cannot have a system where you have that option, that your communication ports are closed when you do not want to use them.
Professor Zittrain: Yes. I have two and a half answers to your question. Answer number one is, you are absolutely right, this is exactly what a firewall is by definition. The computer has different ports. These are virtual constructs but the computer can come to understand them, and the firewall says, "I'm not going to let any data out of these ports except only these other ports and I'll only allow data in if I see that it has been invited by a previous communication out by my own port." So if I see my computer send a signal to a web page and say to the web page, "Call me back on this port," I'll then open it because of that invitation. That is why firewalls, to the extent that they are effective, can be effective. It is also why, I completely agree with you, in the short to medium term Internet service providers are in a good position to detect traffic patterns that are machines which appear to have slipped their leads, precisely because of the way, and the volume, they are communicating. There is the off-chance, when you have a million machines, even a small percentage will represent a good absolute number of people who have some reason to be communicating that way and we could see them being able to say, "No, no, it's fine," but in the short term I think it would be very helpful. Now, on the other hand—and here is the half—firewalls themselves are not cure-alls and a way to understand that is, you may remember the era of cookies, when people were very worried about cookies and their browsers, and browsers responded to the market by giving you an option to individually approve every cookie that is about to be set. It turned out that setting cookies is so useful, especially to support the multi-billion pound advertising economy, that cookies are getting set all the time and if you do set your browser for that you are asked in a way in which you have no way of making an informed decision to accept every ten seconds one cookie or another and it becomes overwhelming. This leads to the second and a half point, which is that a number of applications now that you may find yourself using only occasionally really do benefit you and others by having a fairly continuous set of communications over the Internet, and I will give three very fast examples. One is Skype. You would think that Skype, to do computer to computer calling, when I make a call, is making the connection and when I have hung up it might as well be disconnected. But it turns out that thanks to firewalls and some other issues like so-called Network Address Translation, tricks are needed to make Skype work. In those cases, Skype uses lots of other people's idle connections to help it route calls from one machine to another. This is a very interesting use of the generative PC and network. If you were to have every Skype machine disconnect whenever it was not in use, from the point of view of the Skype implementation it would be a selfish thing to do that would actually bring down much of Skype as a network, and that feature is exactly what the people who made Skype (who are also the people who made Kazaa) are now putting into Joost, which is IP television routing around the bottlenecks of traditional television networks—but they are only able to make it work because they can harvest the so-called grid computing. So just as with so many of these applications, they start off obscure and then enter the mainstream, I think peer to peer computing starts off obscure, grid computing to help chart hurricanes or to look for extraterrestrial life, and then they become very mundane to help Skype or Joost do their thing, or the very definition of "end point" turns out to be flexible. I have one Ethernet drop in my house, but using a service like a phone or something else I might find it socially valuable, and others would too, to share that connection and from the point of view of the ISP they do not know from which computer behind that access point there is use taking place and if I turn off my computer the way I turn off a car when I am not driving it, everybody dependent upon my connection now loses the ability to connect.

Q989 ***Chairman:*** I would still argue that the individual should have the option of not having their machine used as a slave, even for Skype.
Professor Zittrain: Absolutely. I think that is right, and in fact I encourage people sometimes to open up one of those command windows, if they are using Windows, or the terminal window in Macintosh, and just type "netstat" and you can see all of your extant network connections, and if you are running Skype

you are communicating with 100 different machines all around the world and you have no idea what data is going into or out of the machine, and frankly Skype has the keys to the kingdom. It is only because we trust the guys who made Kazaa that we choose to run it.

Q990 ***Earl of Erroll:*** Is there not a big problem, though? If people are only paying for limited band width, then they are actually potentially paying for that Skype connection as well?
Professor Zittrain: That is true. To the extent that the economics of network connectivity turn out to be that one pays in a metered fashion—and that tends to be more typical, say, in the UK than elsewhere—you have got that one gigabyte limit, or something, the act of sharing one connection can end up exceeding that band width.

Q991 ***Earl of Erroll:*** And therefore the users are inadvertently charged for the thing they did not think they were using?
Professor Zittrain: I think that is true, and that would certainly help to at least inform the user, "This is the amount of usage you have," just like it is good to know how many minutes have been used on your phone, especially if you are lending it out to people all the time.
Chairman: We have to move on. Lady Sharp, please.

Q992 ***Baroness Sharp of Guildford:*** Really on the same sort of topic, you kind of argued in your evidence that to achieve the full potential of the Internet it is necessary to ensure that individuals know how to keep themselves safe online. How effectively do you think we as a society are instilling this knowledge, whether into the young or those of an older age, and is it really feasible (as you do suggest at one point) that they should train the kids to teach their grandparents?
Mr Cormack: I did not teach my grandparents. I taught my parents how to use it safely and that was fairly painless. That we are getting there is possibly overstating it. There is a number of very good things happening. There was a QCA proposal on curriculum for key skills in schools, for which I expected to have to re-write huge sections of the draft. I did not. It was all there. I think the only two things missing were the ability to recognise deceptive communication and the ability to maintain your own computer; to run antivirus, to keep it up to date, those sorts of things. Other than that, that was all there, so the curriculum can exist. Getting teachers, not just to teach Internet security one hour a week but to themselves behave correctly, that is hard. There is a nice series of websites and DVDs produced by Childnet, which is the cross-generation thing. There are lots of good initiatives happening. I did spot a Symantec figure which suggests something has improved because in 2004 twenty-five per cent of all the botnet infected computers in the world were in the UK. Last year we were down to four per cent.
Professor Zittrain: Probably more computers, just more other computers!
Mr Cormack: Yes. I could not find the absolute numbers.

Q993 ***Baroness Sharp of Guildford:*** Can I ask a supplementary to this? We understand that many experts ignore advice about encrypting wireless networks and are not in favour of changing passwords regularly, yet these are regarded as being the basics of good security practice. There must be some advice that everyone agrees upon, but how can normal users tell what is good advice and what is not good advice?
Mr Cormack: Run antivirus and keep it updated. Run regular patching, Windows update, or whatever. Turn on a firewall, both inbound and outbound, and be as suspicious and as cynical as you are in the real world. Do not suddenly become innocent and trusting when you go online.
Professor Zittrain: I think that advice is difficult to quarrel with, but it also to me expresses the gap between where we are with the state of the art in advice to the mainstream users and where we need to be if they are not to ultimately migrate away, and for that we really do need—it might be a little bit too colourful to call it a Manhattan project, but we need to recognise that the market did not provide for the Internet to begin with. The market provided networks, but they were these proprietary networks. Government subsidies to academia and interested moonlighting commercial entities and research arms did the trick, and then the commercial forces came in to smooth off the rough edges; a very nice two-step. I think we are in the same situation right now, that subsidising a set of tools which do not exist right now but which could be brought online to actually use the generativity of the Internet and PC to create new tools can help us give, in the long term, much better advice to users. Just one quick example of that is a tool that users can download and it would measure certain vital signs off the machine. It is not hard to say how happy the machine is. How often is it re-starting? How many pop-up windows over a time interval is it getting? There are certain metrics you can gather and then compare with other machines in the herd. You are on a network, you can query nearby machines, so that when you encounter new code, just like a new cookie, seamlessly the computer can say, "Has this code been seen before? Has this code been floating around the network for two years or did it just pop up yesterday, and for those computers on which it is already running, did their happiness levels as machines drop, stay the same or

go up?" Those are the kinds of instruments which could go onto a dashboard which could help users make informed (but not overwhelming to them) choices about what code to run, and it would be respectful of different levels of risk tolerance for different users. What you might choose to run at home would be different from what a merchant might want, or a cyber café owner, et cetera. It is not one-size-fits-all. So I would love to see some money and some momentum put behind the collective development and experimentation with those tools.
Baroness Sharp of Guildford: Thank you.

Q994 ***Lord Harris of Haringey:*** We are about to hear from Ofcom and I know that you have already talked about the sort of "removing road signs" model, but I want to ask you how effectively do you think the Internet security is regulated in the UK, and in particular do you think Ofcom takes regulation of the Internet services seriously enough and are the provisions of the Communications Act (which exclude the regulation of content from Ofcom's remit) sustainable in the long-term, particularly in the context of convergence?
Professor Zittrain: One of the real blessings for me of having taken up residence in the UK now much of the year for two years has been to come to know the staff and the people at Ofcom. The kind of ability I have seen with Ofcom staff to take a sober view of what is going on, the curiosity that I see, the intellectual curiosity that I see that they possess to what is going on and the appropriate level of caution with which they treat interventions they might be in a position to make, all of those to me bode very well. I think content regulation is a briar patch that they would not want to be thrown into because, especially once you go there and have to start making truly content-based decisions, security is now a side issue, at least technical security, and it will be much harder to devote attention to. So this is not a paean to inaction, but I think so far Ofcom has been keeping an eye on the situation, understanding that the interventions are delicate enough right now that they require cooperation from a lot of parties. There is not just one regulatory point of intervention that can solve the problem.
Mr Cormack: I had interpreted the question differently. I think I would agree with your possibly unstated thing, that regulating content is going to be incredibly complicated because it is so hard. Regulation automatically involves drawing lines and defining where those lines are. We have recently been looking at IP television and when different licensing regimes come in, and the question appears to be how much delay from the original broadcast there is. That is a completely arbitrary decision which is going to be made and wherever you draw the line people will either be one second ahead or one second behind. The impact of that, actually defining something, I think would be highly disruptive.

Q995 ***Lord Harris of Haringey:*** Can I just finally ask about the sharing out of responsibility between Ofcom and the Information Commissioner. Do you think that works satisfactorily? Should the Information Commissioner be given more teeth?
Mr Cormack: I would certainly be very pleased to see the Information Commissioner able to deal more effectively with particularly spam, which I know is a concern of that office. It is interesting that in the past few months it has become apparent that actually the most effective way to deal with spam in the UK is through the civil courts, not by the regulator at all, which is really rather depressing.
Professor Zittrain: I cannot yet share a useful answer to that question, given my own comparative ignorance of the governance here.
Lord Harris of Haringey: Thank you.

Q996 ***Chairman:*** We are nearly at the end. There is one very quick question and I would like a very quick answer. Is there a problem with researchers crossing the law when they are researching these topics?
Mr Cormack: As of today, no, because the amendments to the Computer Misuse Act (1990) brought in by the Police and Justice Acts 2006 are not yet in force. I think as currently drafted and lacking further explanation, I have had a lot of concerns expressed, not just by researchers but by teachers, asking whether they have to stop undergraduate teaching where they are teaching people to code securely by getting them to write an Internet server and then exposing that server to hacking tools. An excellent way to teach programming, but they are saying –

Q997 ***Chairman:*** It is a good way to teach hackers, too?
Mr Cormack: No, but to teach undergraduates to actually think about security when they are coding, which is all too rare in professional programmers, by clearly demonstrating what happens if you do not, exposing it to the typical background noise of the Internet—right through to people who are at masters level, teaching penetration testing as professional development. They have contacted me, saying, "Do we have to pull this course next year?" My current answer is, "I am afraid I don't know."

Q998 ***Chairman:*** We are going to have to bring it to an end. Thank you very much indeed. You can sense our interest in this and we do not have enough time, but we never have enough time when we really get interesting witnesses. So thank you very much indeed for your contributions. If you think of anything else which you think might be useful for us, please let us know.

Professor Zittrain: Thank you.

Mr Cormack: The thing I had forgotten halfway through was that if an ISP takes action to degrade or modify a user's connection, they must provide the user with information so the user can fix his own problem.

Chairman: All right, we note that. Thank you.

Supplementary letter from Andrew Cormack

Thank you for an interesting and stimulating afternoon at the inquiry on Wednesday. Apologies for my confusion over Lord Harris' question on Internet regulation. I had thought of the issue in much more general terms so the specific focus of the question on Ofcom threw me. I hope I may take up the Committee's invitation to submit follow-up observations to say now what I had intended to say in my witness evidence.

We already have a number of pieces of legislation that could be used to regulate Internet activity but, as yet, very little use of these by the authorities or the courts. I believe there have been fewer than 100 cases in 17 years of the Computer Misuse Act 1990, a handful of civil cases against spam under the Data Protection Act 1999, just two that I know of under the Regulation of Investigatory Powers Act 2000, and the provisions of the new Fraud Act and Police and Justice Act are untried. So I would like to have more experience of the use and effect of these existing regulatory powers before considering what, if any, additional regulation might be needed.

This seems particularly important because the balance of regulatory incentives is so delicate and the risk of unintended consequences so high. The current notice and takedown regime for content (implemented as the Electronic Commerce (EC Directive) Regulations 2002) was criticised by the Law Commission in December 2002 for encouraging ISPs to remove without question any and all material that was the subject of a complaint. Current regulation makes it legally hazardous for the ISP to act in any other way and a Dutch study did, indeed, discover that the majority of ISPs responded to bogus copyright assertions by removing the material from publication without question. As the Law Commission commented, this is an unhelpful power to restrict freedom of speech on line.

Any imposition of liability for unusual traffic would have to be drafted extremely carefully to avoid creating a similarly one-sided incentive to cut off the Internet any device that deviated in any way from the normal pattern of traffic. On JANET we are currently struggling with a research platform called Planet Lab which allows researchers to experiment with new ways to use and measure the Internet. Planet Lab hosts frequently trigger our "hostile traffic" alarms and we spend a great deal of time investigating what almost always turn out to be beneficial, but innovative, experiments. A year ago we would have had the same issues with Skype traffic; some time before that it was the emergence of peer-to-peer and grid applications that was 'unusual, maybe hostile'. As a Research and Education Network we feel a moral duty to support innovative use by fully investigating any anomalies and only disconnecting once they are clearly harmful, but if this duty were set against a potential legal liability then it would be very hard to sustain our current practice. "Mere conduit" status protects experimental applications as well as ISPs.

Sudden changes in traffic patterns, known as "flash crowds", have always been a feature of the Internet and are often a sign of healthy innovation. Regulation that presumed, by imposing one-sided liability, that all flash crowds were hostile would run a serious risk of freezing patterns of Internet use as they are today and making the Internet inimical to the innovative developments required to create the applications of tomorrow.

20 April 2007

Letter from Ofcom

During the oral evidence session on 24 January as part of the Committee's current inquiry into Personal Internet Security, reference was made to comments by Professor Ian Walden from the Society for Computers and Law, who said that Ofcom, with its good reputation and better levels of recognition, would be well placed to offer regulation in Internet security. Ofcom also notes thae recent report published by the Society for Computers and Law which states at paragraph 17 that "Ofcom is the proper person to enforce Regulation 5 of the Privacy and electronic communicatiosn "ePrivacy" Regulations (PECR) and not the Information Commissioner".

While Ofcom is appreciative of Professor Walden's kind words in Committee, as he later recognises in that discussion, Ofcom does not have a remit in the wider area of personal Internet security, or indeed the necessary expertise. In relation to compliance with PECR as the Society for Computers and Law suggests, while Ofcom does have certain powers in this regard, Ofcom and the Information Commissioner's Office (ICO) are shortly to finalise a letter of understanding which sets out the basis for future collaboration between Ofcom and the ICO in areas where we share a common enforcement responsibility.

At present, these areas are primarily those covered by the PECR—which include the use of automated calling systems, the transmission of recorded messages that contain direct marketing material, and compliance with the Telephone (TPS) and Fax (FPS) Preference Services.

As the Committee will know, there are areas where Ofcom or the ICO will have specialist experience and might generally be expected to take the lead. Examples might include where the issue of privacy is foremost and the ICO would be expected to take the lead. In contrast, if an investigation would benefit from technical knowledge of the communications sector, Ofcom might be best placed to take the lead. Ofcom notes that the ICO has recently undertaken enforcement action in compliance with the TPS scheme. A link to the ICO's press release in its December enforcement action can be found at www.ico.gov.uk/upload/documents/pressreleases/2006/en__6__dec__06.pdf.

It is also worth noting Ofcom's recent enforcement action imposing a financial penalty of £10,000 on 1RT under section 130 of the Communications Act 2003 (penalties for the persistent misuse of a communications network of service) in relation to their sending faxes containing marketing material to telephone numbers registered with the FPS without consent, details of which can be found at www.ofcom.org.uk/bulletins/comp__bull__index/comp__bull__ccases/closed__all/cw__891/.

Ofcom considers that such an understanding supports appropriate enforcement, providing clarity on the roles of the two organisations and playing to the expertise of both.

8 March 2007

Examination of Witnesses

Witnesses: MR TIM SUTER, Partner, Content and Standards, MR BEN WILLIS, Head of Technology Intelligence, and MR JEREMY OLIVIER, Head of Multimedia, Ofcom, examined.

Q999 ***Chairman:*** We are sorry to have kept you, but you have been listening to the conversation, no doubt, so you see our interest. Thank you very much for coming along, Mr Suter, and for bringing your colleagues. Perhaps, as with the previous witnesses, you would introduce yourself, please, and have your colleagues introduce themselves.

Mr Suter: Thank you very much, my Lord Chairman. My name is Tim Suter. I am the Ofcom partner responsible for content regulation and in that capacity I am also responsible for our programme of work in relation to media literacy, which is a subject I suspect we will want to cover a bit. On my right is Ben Willis, who I will ask to introduce himself.

Mr Willis: I am the head of technology intelligence in Ofcom, so in that role I take an overview across some of the technical issues which are going to confront us in our regulation and in particular I do some of our liaison with the Government on security related matters.

Mr Suter: And on my left is Jeremy Olivier.

Mr Olivier: I work, like Tim, in the content division of Ofcom, but specifically focused on the evolution of content regulation, where it is going and how the Regulator may respond to some of the developments we have been talking about today, for example in relation to the Internet.

Q1000 ***Chairman:*** Thank you. Let me open with the first rather general question. Who regulates the Internet and Internet services in the United Kingdom?

Mr Suter: I think our opening response to that is that the Internet as an issue in itself needs to be separated out from the services which are regulated, and to the extent that services are regulated the Internet is one means of carriage of those services, and where they are services which fall to be regulated they are therefore regulated by the appropriate regulator. For instance, if you take the example of IPTV, the fact that it is carried using Internet protocols does not prevent it being regulated by us in the same way that we regulate other traditionally broadcast methods of TV, whereas other forms of content which are delivered online using the Internet, because they do not share the characteristics of television in the sense of their simultaneity and their availability to the general public (as set out in the Communications Act), are not regulated. They are both carried by the same means but it is the nature of the service to which the regulation attaches itself rather than necessarily to the Internet itself.

Q1001 ***Chairman:*** That is interesting. The supplementary question I would ask is that Ofcom was excused from regulating content on the Internet,

but you are saying it is not really, are you not, but it does regulate electronic communication networks? How does Ofcom regulate this area in practice? I guess you have just given us part of the explanation of this.
Mr Suter: I hope so. Perhaps I could elaborate and in the process perhaps pick up some of what Lord Harris was getting at, I think, in his questions about the future, and certainly Professor Zittrain's response. The key issue which drives content regulation, if you deal primarily with content regulation, is audience expectation. That which gives us the purchase to regulate content is the expectation on the part of the audience that there is a safe environment, an environment where an external body takes a view and operates in a backstop capacity. Those services will have certain characteristics. They will be part of a linear schedule, they will be delivered simultaneously to everybody and the mere fact of choosing whether or not to avail yourself of the service will not prevent that piece of content being delivered at that time, because as a content regulator that is what I need in order to take a view on a given piece of content. A piece of content on its own has virtually no meaning until it is viewed or consumed by somebody in a particular context. Without the context, the content alone means very little to me. A piece of adult content on its own, without knowing who consumed it, when they consumed it, how they consumed it, with what protection preventing them from consuming it means nothing to me. If I know that it was broadcast on a channel which was heavily protected by a couple of PINs available only late at night on a subscription service, that is one thing. If I know that it was broadcast free-to-air at four o'clock in the afternoon, that is different, but it is the same content. So the context is the element which is key and therefore the audience expectation and the context is what gives us our legitimacy to regulate content.

Q1002 ***Lord Young of Graffham:*** So what you are telling us really is that IPTV comes under your controls, the content of IPTV?
Mr Suter: Where IPTV is essentially transmitting the same broadcast stream which is being transmitted elsewhere using other means, via cable or satellite.

Q1003 ***Lord Young of Graffham:*** If I take one of those programmes and put it on as a video podcast, that is out of your control?
Mr Suter: That is out of our control.

Q1004 ***Lord Young of Graffham:*** But it is the same programme?
Mr Suter: It is entirely the same programme, and indeed at the moment you will be able to watch on your screen, the same screen, the same piece of content which will be regulated by a variety of different means. A piece of video on demand –

Q1005 ***Lord Young of Graffham:*** What is the point of trying to regulate IPTV if it is the same programme in some way, looking at the content of IPTV? If exactly the same programme is deregulated or is outside regulation, if it comes down not on a constant stream but by way of a video podcast?
Mr Suter: If I could start, and then I will ask Jeremy to pick it up. The key issue is the nature of the service to which the regulation is attached. The service has a certain contract, if you like, with the viewer which says, "Within this service we will abide by certain rules. Up to a certain point you need take less responsibility in regard to what your children are going to watch, but after a certain point you need to take more." There is, if you like, a regulated contract which can apply to the nature of the complete service. Within that, we can take individual judgments on pieces of content. A piece of content that is entirely dependent upon my individual choice, when to go and get it, where to consume it, how long to store it for has a different set of issues attached to it, and therefore the kind of broadcast regulations which we attach to linear IPTV services would not be appropriate. Jeremy?
Mr Olivier: I think you have made the point I was going to make.

Q1006 ***Chairman:*** Could I just test that one? If you are a school teacher, a nasty, bad school teacher, and you have a subscription service which you only have access to at night and you were to record a nasty movie and then play it to your class of ten-year-old children the next morning, is that against the law?
Mr Suter: I think it would depend upon the nature of the content. It certainly would not be against the Broadcasting Code.

Q1007 ***Lord Young of Graffham:*** Some of these video podcasts, for example, get pushed out on a regular basis at ten o'clock every Thursday morning, a specific time, or something like that, down to a PC and it becomes really indistinguishable from broadcast television, does it not?
Mr Suter: I think that is why you have to separate out the nature of the service which is delivering it from the nature of the consumption. If you take a piece of content, you can watch it at exactly the same time on exactly the same screen as a regulated piece of content. The same film may appear being broadcast at eight o'clock and you may watch at eight o'clock the same piece of content you got from a podcast. That does not in itself undermine, to my mind, the notion that in one environment you have a regulatory environment which says, "This is a linear schedule. Certain rules will apply," and in the other you have

chosen to go and get that specific piece of content which you happen to watch at that time. No editor took responsibility for putting it out at that time. The editor of the podcast did not decide this was an appropriate environment within which to consume it. That consumption decision was yours.

Q1008 ***Lord Young of Graffham:*** This distinction might be in law or in the Act. Do you think it will last?
Mr Suter: I think it will be reinforced. I think it is there now and I think it will become more important. I think we will see broadcast regulation, if you like, the kind of broadcast regulation which we currently apply to a whole range of channels. I think that will still be there because I think there is audience expectation and I think there is a very considerable degree of consumption of programmes delivered in that way where people want the confidence of that environment, but we will see increasingly content being consumed in other ways.

Q1009 ***Lord Young of Graffham:*** Are we not moving away from broadcast television to an era in which people choose what they want to see when they want to see it?
Mr Suter: And as that happens the industry will need to develop its own self-regulatory approaches, its own self-regulatory mechanisms for providing that reassurance.

Q1010 ***Lord Young of Graffham:*** But as we go from one which is controlled, we go to the other which is not controlled?
Mr Suter: It is self-controlled.
Lord Young of Graffham: Yes, that is right.
Chairman: We will come back to that in a minute. Lord Mitchell, let us have your question. We are going to come back to some of these topics.

Q1011 ***Lord Mitchell:*** What risks to personal Internet security can arise within the networks themselves?
Mr Willis: I guess the first point I would make there is that it is slightly difficult to distinguish, to draw a hard line between the network and the people who use the network around the edge. So the network of itself is not capable of doing bad things. What the network can do is have weaknesses in it which create the holes which bad people can come and take advantage of. I guess the way I understand the question is, if we are assuming that the end users have done everything in their power to ensure that their computers are patched, that they have all the right virus protection and that they are not doing anything silly themselves, what risks can they be put to by the actions of the network and the network operator? As I say, I think that is merely opening the way for a third party with criminal intent to come and take advantage of those weaknesses, if you like, to actually exploit security. There is a whole number of ways in which that could happen. Just to give an example of some of the weaknesses that we might see, one is vulnerabilities in the network which have not been patched by the operator. They, for example, might be bugs in the software that run on the pieces of equipment that make up the network which the operator has not done anything about but which somebody comes along and exploits. So they write this code which attaches itself to the network devices and then can interfere with the security by stealing their details, for example. There is a number of reasons why that situation can occur. Firstly, because it is a bug which the hackers became aware of, either in advance or at the same time as the vendors of the equipment, and at the moment the vendors of the equipment have not yet come up with a solution for that bug so there is nothing the operator could have done about it, i.e. there is no fix for this problem which is being exploited by somebody else. The alternative is that the vendor has created a solution to this bug and the operator simply has not installed it yet. That case is particularly unlikely. It is a matter of course for operators generally to be in very close communication with their vendors, much more so than the average computer user, to keep their network patched and up to date. There is a couple of other examples. We could find, for example, that communication which the user sends across the network gets intercepted at some point on the network. Again, there could be a couple of reasons for that. It could be because the security on the network, either the physical security or the electronic security, has been breached by somebody, so somebody has broken into an office of the operator and attached their computer to the network and sees the traffic going across and can intercept credit card details, or it could be because that network was not secure in the first place, it did not try and stop people from stealing stuff. The other kind of source of these things, which is probably far more likely in practice, is basic human error or problems with the processes and procedures operated by a network operator. So it could simply be that somebody loses a laptop which has customer details on, or that the processes within the network operator lead to them inadvertently exposing lots of personal information to other people. I guess the final example I was going to give is the criminal activity by an employee of a network operator, where somebody working within the network actually steals personal information. So there is a number of ways in which even if the end point has been properly secured—and as we said earlier, that is far from a given—the network itself could still present risks.

Q1012 ***Lord Mitchell:*** Have you been made aware of any risks to personal Internet security arising from within the networks themselves?

Mr Willis: It is an area which we do track and take notice of. I guess in general it is not something which falls directly under our control.

Q1013 ***Lord Mitchell:*** But have there been specifics?
Mr Willis: There are specific examples.

Q1014 ***Lord Mitchell:*** What sort of actions do you take?
Mr Willis: I am not aware of any examples which have fallen to us to take any action on. A fairly recent example, for instance, is that there was an attack on the Internet infrastructure, quite widespread, a global issue, which came through a security weakness in a piece of software which was run on some of the main Internet routers and this was taken advantage of and they were attacked. The operator community was aware of this as it was happening and worked to fix the problem as soon as possible. It was not something where any regulator intervened to fix it, it was fixed by the industry before it became a compromising problem.
Lord Mitchell: Thank you.
Chairman: Lord Young, we talked about this topic, but I think it is worth asking your supplementary question.

Q1015 ***Lord Young of Graffham:*** Yes, because I would like to actually test it, if I could. You argue in your memorandum that the distinction in the Communications Act between "content services" and "electronic communication networks" is "quite clearly defined". Do you think this distinction is going to survive in the long term?
Mr Suter: I am going to ask Jeremy to lead off on that.
Mr Olivier: I think, in the light of the discussion we have had to date, I will answer the question slightly different than I had originally anticipated doing so. In the Act there are two distinct things defined, as we said in our evidence. One is an electronic communications network, which is a means of delivery of an enormously broad range of services, and another is a content service, and the definition of content service focuses very explicitly on the provisions, on agency and the provision of content of one kind or another by a service provider, by a content service provider, to a consumer or a set of consumers. The reason why that is important in the Act is because, as Tim was explaining, there are some types of content services described in the Act as "television licensed content services", which has certain characteristics. They are made simultaneously available to very large numbers of users, they are potentially impractical, potentially harmful in some instances, particularly to minors (that is a key area of concern), and which therefore we have a special regulatory architecture to oversee. If your question is—and I think perhaps it is—"Do you think there is a future for the regulation of some types of content service in order specifically" (as we do currently) "to protect vulnerable individuals against exposure to harmful and offensive content," I think the answer is that absolutely there will continue to be such a role. It is very unclear, to me at least, that there is much appetite among audiences for a move away from the provision of some degree of security of the kind you have described. Indeed, in the questions you were asking Professor Zittrain there seemed to be in some sense that you were exploring options for creating such a regulated domain in relation to other security issues by taking responsibility away from where it sits presently with consumers—they are responsible for putting the firewalls, and so on in place—onto ISPs. My analogy would be that we currently have a content regulatory architecture. We believe the audiences value it and that therefore there is strong evidence to suggest that there will continue to be a role for such an architecture.

Q1016 ***Lord Young of Graffham:*** Let me just test it. The technology is moving so that PCs and televisions are merging into media centres, and indeed your PC and your television will be connected by wireless. So we have programmes which at the moment have to go out after the watershed, after nine o'clock in the evening, which the following day can be accessed at any time of the day as a podcast. So one gets regulated. What is the point of having a watershed at nine o'clock if the same programme can be accessed at any time?
Mr Suter: That has been the case, I think, since the invention of the video recorder. Time shifting material has always been the case. So the fundamental principle is not, do we prevent material being accessed by people? The answer is no, and anyway we are an after the event regulator. The fundamental issue of content regulation is to provide tools and information to consumers which say, "If this material is broadcast at a certain time or on a certain channel, or with a certain degree of additional warning or preparation, then you should take note of that." We do not assume that the nation's children are in bed by nine o'clock. We know that they are not. The notion of the watershed is not because we believe children are in bed, it is because we know that consumers need a signal which says the level of responsibility shifts at a certain point in the linear schedule, and actually the point is different according to different kinds of channels. So it is not that there is an absolute prohibition or the intention to prevent that material ever being seen. We would rather that it was not. What there is is an intention to give people the tools they need to manage their own consumption. In a regulated linear environment it is

relatively straightforward to do. In a non-linear environment it is much more difficult to do in the old way, so you need content information, you need consumers to know, "What is it that I'm getting? With what degree of caution should I approach it? With what degree of care should I manage who's watching it?"

Q1017 ***Lord Young of Graffham:*** So you could see Ofcom changing the regulation in order, perhaps, to put up a warning signal for these post-watershed periods being broadcast at any time? If the whole idea of regulation is to help to guard young children from seeing unsuitable material, then what happens with time shifting where, whichever technology it is, it is available at any time? The big difference with time shifting with a VCR of some sort is that it is a positive act to do it, but with the other one people can roam around the Internet and come across them in different ways, I think that is the real thing, or subscribe to them?
Mr Olivier: I think there are a number of points to make in response to that. Perhaps the first and most simple is that, as we have been discussing, Ofcom does not, I think, anticipate that we would be able to impose global standards either for labelling or for any other form of content regulation to the global medium, that is the Internet, but that does not at all mean that it would not be desirable (as in fact we are already doing) to seek to work with those service providers who are legitimately available to us as partners in delivering content regulatory outcomes and that they should work to provide audiences with appropriate tools to enable them to manage their and their children's access to content. So not necessarily regulating in the way that we do with broadcasters but certainly working with service providers, as we do currently, to help them make these kinds of tools available to audiences and thereby to delivery the goal that we share, I think, which is the protection of vulnerable individuals in this particular instance.

Q1018 ***Earl of Erroll:*** You state in your written memorandum that "Although security products are valuable tools for consumers they are not a part of the regulated Internet access service". Can you explain this distinction in more detail?
Mr Suter: I shall ask Ben first to explain that.
Mr Willis: I guess the first point is that in the sense that those security tools generally are pieces of software which would run on a consumer's PC they are not part of the service which is offered by the operator per se, they are something in the customer's domain and therefore outside of what we would think of as the regulated Internet access service itself.

Q1019 ***Earl of Erroll:*** They could be actually part of the service, and I think that is the point, because the business of ISPs is to provide the customers with access to the Internet and some of it is the information it holds. There is also the other side, which is email, and there is no technical bar to them making those services safer. For instance, in the Lords we use MessageLabs to filter our incoming email before it hits our mailboxes in the Lords, so it would be quite easy for ISPs to do this sort of thing. Why are they, unlike companies in all sorts of other walks of life, not required to provide their services with due regard to the security and safety of the users?
Mr Willis: I think the answer to that is that there is a number of aspects of the service which we do regulate and then a whole bunch of other things which the ISP can choose to add or not, which we do not regulate. The parts which we do regulate are set out in what are called the General Conditions of Entitlement, so they are the instruments of regulation for services and networks. They cover things like customer contracts and how a customer would be billed, how disputes would be resolved between customers and operators and how customers would be migrating between providers. Those features are the things which come under our regulatory remit to control. Other things which an ISP may choose to add to the service, for example, "We will filter your email for you," or, "We will offer you a whole bunch of other services," are outside the things which we regulate under that framework.

Q1020 ***Earl of Erroll:*** But in general Government tries to protect its citizens and also provide a good environment for business to operate in and for citizens to live in and providing that security for society is part of our responsibility, one would feel, and yet this does not seem to be part of your responsibility, to try and make it a more secure environment for consumers or users on the Internet. Do you not feel it should be, perhaps?
Mr Willis: At the moment there is a review of the framework which governs these things going on in Europe at the moment, as I am sure you are aware, and one of the things that review is looking to do is to extend the framework in these areas to cover more of this sort of activity. You can come up against a number of problems. One relates back to the example of the moving of the road signs. There is the potential that if end users feel the security and safety responsibility is not with them any more, that the network will look after them, that reduces the likelihood and the ability of the users to take responsibility for their own actions and there is only a certain degree to which the networks can ever protect the end users. We have also concerns over putting in place hard wired regulations to cover those

things. The framework is not desperately old, but it could not have been possible to have pre-empted a lot of the problems we are now seeing when that was written and hard wiring this into regulation is not likely to be a very effective method. So it would be very difficult for us to write down, for instance, what it is we would expect the ISPs to do specifically, and it would change day by day.

Q1021 ***Earl of Erroll:*** So you have been effectively working on the Code of Practice with the ISPs? That is what I gathered you were saying?
Mr Suter: No. There are the Framework Directives, which are the European governing frameworks, which are currently under review in Europe.
Mr Willis: And they govern which aspects of the service we do and do not regulate.

Q1022 ***Earl of Erroll:*** Right, but you are not talking to the ISPs about trying to do something of that kind?
Mr Suter: Where we are talking about, for instance, labelling and information, then we are indeed talking to content providers, but in the context that this is a service they can provide to consumers rather than one we mandate.
Mr Olivier: I think it is worth adding that in relation specifically to the question of how Ofcom is working to improve consumer security our focus and attention has not been on trying to force ISPs to take on that responsibility in a traditional kind of bilateral industry regulator model, but rather on helping ensure consumers are effectively enabled to take on that responsibility themselves, to run their own firewalls, and so forth. It is for that reason that Ofcom participated in and part funded an initiative to develop a kite mark for filtering tools in the UK, which I think is largely complete but the marketing of which has not yet launched, but the objective of that is to enable audiences, consumers, to have confidence in adopting tools which will, for example, enable them to protect their children against harmful or offensive content more effectively.
Mr Willis: I think there are other examples of that in the written response as well.

Q1023 ***Chairman:*** You do work with ISPs to try and fix the problems and despite firewalls and despite antivirus software a hell of a lot gets through. Phishing is going on, it is alive and well, and so is quite malicious spam, so presumably you sit down with the ISPs and see if you could not figure out a way to stop this?
Mr Suter: I think the important answer is that we certainly want to understand the actions which are being taken by those who can prevent it, but we do not see it as our role to prevent it.
Mr Willis: Yes, I think that is right and there is no simple answer to these problems. I think the industry is moving in the right direction and there is a lot more which is being done. There is no perfect answer and it is not because somebody knows what it is and they are not bothering to do it, it is an ongoing arms race, if you like, and I think it will always be that.

Q1024 ***Chairman:*** But are you saying it is not your responsibility, even if a perfect answer to filtering the content, for example, was discovered, that that should be implemented? We would all like not to receive phishing emails or malicious, unpleasant spam. It might seem to us that it would be your responsibility, should a solution exist, to ensure that that solution was implemented?
Mr Suter: I think we would see our responsibility, certainly, as understanding what those who are responsible for delivering the solution (which in this instance we would see as being those providing the service) ought to put in place and encouraging them to do so, and working with consumers to make sure they are aware of all the protections that are available.
Chairman: All right, let us move on.

Q1025 ***Baroness Hilton of Eggardon:*** You have a role, I think, in developing media literacy, do you not, in the population? Do you think that part of that is ensuring that people understand what they should do in relation to the Internet to make them safe and secure, and so on? Is that part of your remit?
Mr Suter: It is certainly part of our remit to help consumers to both access and understand the communication services which are available to them and that will include making sure, as far as possible, that they know of the tools which are available to help them manage that environment in a way they want to manage it.

Q1026 ***Baroness Hilton of Eggardon:*** So how do you set about doing that?
Mr Suter: The first issue we have tackled—and I think some of the evidence is in our submission to you—is at least establishing a base of where we are. Where can we feel confident? Where do we think there are issues? Are they in relation to particular age groups? Are they in relation to particular activities? Are they in relation to particular bits of awareness? I will not go through the details because I know it is all in the memorandum which we supplied, and we will be very happy to supply you with the much more extensive media literacy audit. It suggests that there is a mismatch between what parents, for instance, think they do to control the environment in which their children are operating and what children think their parents do to control that environment. You might expect there to be a mismatch. It may not strike you

as large, it may strike you as worrying, but nevertheless there is a mismatch. Parents think they apply the rules; children think they do not. So we have to understand, first of all, what is the environment that people are working in, and then to understand what are the most effective tools we can offer. As I think we have talked about at some length already, one of the key issues is giving people information about the content they are about to consume so that they can make a choice, giving people information about the kinds of Internet protection which are there, which is the work we have been doing with the Home Office on the kite mark. Our work on the audit allows us to focus on what are the key issues we ought to tackle.

Q1027 ***Baroness Hilton of Eggardon:*** Yes, but your audit is just about understanding, it is not about actually taking actions to inform people?
Mr Suter: Indeed, and our duty is to promote rather than to enforce.

Q1028 ***Baroness Hilton of Eggardon:*** I did not say "enforce", I said "inform". Are you actually doing anything to inform individual consumers?
Mr Suter: Oh, I hope we are doing something to inform, certainly, through the kite mark programme. That will have a very wide availability and it will be marketed very widely, and I think that is an important thing that we will do. That is playing our part, if you like, to inform consumers of what is there, working with those content providers to ensure that they inform consumers about every piece of content they might be about to consume. This is indeed information.
Baroness Hilton of Eggardon: Thank you.
Chairman: Lord Harris, you touch on this in your question.

Q1029 ***Lord Harris of Haringey:*** Section 14 of the Communications Act requires you to conduct consumer research, for example, into the experience of consumers in purchasing electronic communications services and you have outlined some of the research in your evidence. What you have not told us is what you have done with the results. Perhaps you could outline that and also Section 14(1)(d) covers other matters "incidental" to consumers' experiences. I would be interested to know how you interpret that.
Mr Suter: I will certainly do the first part. The second part I will invite Ben or Jeremy, if they want to, to come in on, otherwise I am afraid I am not sure that I will be able to give you a full answer and I might have to write to you on that. In terms of the first part, indeed the consumer experience research gave us quite a broad understanding across the piece of the consumer experience and allowed us to identify three things where we thought we ought to take action. The first was around mis-selling and slamming, the second was silent calls, they were a considerable concern to consumers, and in the third area there were issues around switching. So we have taken action in relation to all three of those. If I just give you briefly the headlines, we started an active programme in 2005 on mis-selling and we have got current investigations against a number of big suppliers there and there is quite a lot of close monitoring that we are doing. On silent calls, I think you will have seen some of the enforcement action we have taken and some of the fines we have levied. On switching, you will be aware, I think, that in the middle of February we introduced new rules around the provision of MAC codes which would make switching easier. This is the kind of thing which our consumer experience research is designed to support, alongside the reflections which it made on people's experience of safety, particularly safety of content online and in particular in relation to their children, which is why we are doing more work now on public attitudes to the regulation of content on the Internet.
Mr Olivier: I am afraid I cannot comment.
Mr Willis: No, I cannot either.
Mr Suter: We will definitely write to you on that.
Lord Harris of Haringey: Thank you very much.
Chairman: A final question from Lord Young on 999 calls.

Q1030 ***Lord Young of Graffham:*** It is a sort of Catch 22, is it not? The voice-over-IP industry tells us that they cannot provide 999 calls because if they do they would be caught by the regulations which apply to wire line, which are quite rigorous and very necessary for that. But in this way we are being deprived of the traditional 999 facilities where everybody is going to avoid them and there are more and more of these going to come. Is that not something you should be looking into?
Mr Willis: Absolutely, it is something we should be looking into, and we are and have been for a number of years in fact. Our duties here are to try and balance the benefits of the innovation and competition that VoIP brings with consumer protection for the 999 services, clearly. We first looked at this issue back in 2004 when VoIP was considerably less important in a market sense than it is today. It was a smaller and more geeky activity. We were aware then of exactly this problem and what we did was we came up with a policy of forbearance with regard to VoIP services. So we wrote a statement which essentially said to the VoIP operators that we would give them a period while the market was establishing itself where we would not enforce exactly the conditions they are referring to here on them if they chose to offer 999 services. What we were hoping to do with that was to try and take away any regulatory disincentives for

offering 999 services, the balance being that it was better to have some 999 access than none at all. Obviously, the ideal is a gold-plated version of 999 access, which we have on the fixed line. We reviewed that and we produced a statement at the end of last month on this, effectively bringing that forbearance policy to an end. We observe that even while that forbearance policy has been active, for the last two and a half to three years, there have been very, very few VoIP operators who have chosen to introduce 999 services even then, but we are aware that with that period coming to an end there are certainly going to be increasing issues for VoIP operators who want to offer these services. With that in mind, what we have undertaken to do is a further consultation on this whole area of voice-over-IP and the availability of 999 services and we are committed to do that consultation during the summer of this year and we will be addressing exactly those issues in that, and that work is already under way.

Q1031 ***Chairman:*** Good. Thank you very much. That is our last question, I think, and thank you very much for coming to answer our questions. It has been very valuable to us. As I said to the others, if you think of anything which you think might be useful to us, please send it to us.
Mr Suter: Thank you, Chairman. We have very much enjoyed the session. We clearly owe you a letter anyway on the Section 14.
Chairman: Thank you very much.

Supplementary letter from Ofcom

At our oral submission of evidence to the Committee on 18 April 2007, we said we would provide supplementary written evidence in response to a question posed by Lord Harris of Haringey.

Lord Harris asked how we interpret our duty under section 14 of the Communications Act to ascertain the interests and experiences of consumers that are incidental to, or connected with, their experiences of communications services. Although Lord Harris referred to section S 14 (1) (d) of the Act, this duty falls under subsection (f).[14]

We fulfil this duty in two ways: consumer research; and engagement with stakeholders.

Research

We carry out a substantial programme of research to explore consumers' interests and experiences that are related to communications services. Our poilcy projects often involve empirical consumer research, and we use a variety of methodologies, from quantitative surveys to deliberative workshops with members of the public.

Some of our research is not tied to a specific policy project, so we can form a broader picture of consumers' experiences and concerns. For example, we carry out an ongoing residential tracker survey, which aims to provide us with a continued understanding of consumer behaviour in UK markets.

Our consumer experience research[15] mentioned in our previous written and oral evidence, will be repeated on an annual basis. This includes broad, open and unprompted questions that seek to explore consumers' concerns, without the research being framed within the context of a specific policy project. Our annual communications market report[16] also contains a significant amount of information on new trends in consumer behaviour.

More broadly, we track changes in consumer demographics and behaviour through additional analysis, including interpreting secondary data (such as Office of National Statistics data on demographic changes). We fund, jointly with other organisations, research on breaking trends in consumer behaviour in communications and other markets, in several countries.

Stakeholder Engagement

Beyond research, we organise an ongoing programme of stakeholder engagement with consumer and disability organisations, to learn from their experiences. Engagement takes a variety of forms, including bilateral meetings, informal email and telephone contact, holding stakeholder events, and attendance at consumer group meetings. We also will pilot an online forum for stakeholders, so that they can discuss issues and provide further input into our work.

[14] Ofcom must make arrangements for ascertaining: (f) the interests and experiences of such consumers in relation to other matters that are incidental to, or are otherwise connected with, their experiences of the provisoin of electronic communications networks and electronic communications services or of the availability of associated facilities.

[15] www.ofcom.org.uk/research/tce/report/

[16] www.ofcom.org.uk/research/cm/cm06/

Their input helps ensure that our work directly addresses the interests of consumers. We also carry out a series of events that are open to the public when consulting on our Annual Plan, to help us assess whether our priorities reflect people's concerns.

1 May 2007

Supplementary Memorandum from Ofcom

How does Ofcom interpret the distinction between "content services" and "electronic communications services", where there is a regulatory function under the Act? What impact is convergence likely to have on such distinctions over time?

The Electronic Communications Service definition in section 32 of the Communications Act 2003 makes quite clear that an ECS consists in the conveyance of signals by means of an Electronic Communications Network but only insofar as it is not a content service.

Section 32 (7) states that "a content service" means so much of any service as consists in one or both of the following-

(a) the provision of material with a view to its being comprised in signals conveyed by means of an electronic communications network

(b) the exercise of editorial control over the contents of signals conveyed by means of such a network.

The distinction therefore is clear; an ECS is not itself a content service, but can rather be the means by which a content service is provided.

A converged environment will increase the potential for delivery of content services via an expanding number and type of electronic communications services. This will mean more operators will be able offer both content services and electronic communications services alongside each other (the most obvious example of this is in the provision of content services (portal pages, etc) by ISPs, alongside their provision of Internet access).

However, we do not expect that this will mean that convergence will make it more difficult to apply the relevant distinctions set out in the Act which as stated above are quite clearly defined.

Is Ofcom engaging with ISPs on the provision of security products (anti-virus software, filtering, firewalls etc) to encourage the development of industry codes of practice?

Regulation of ISP Provision

Although security products are valuable tools for consumers they are not a part of the regulated Internet access service—any more than are the PCs which are typically used as the access device. Antivirus software, firewalls etc. largely run on customer equipment and are in practice outside the control of the Internet service provider (although AOL provides filtering services on its network as a value-added element of its service to subscribers, other ISPs do not).

However, Ofcom welcomes the fact that most ISPs and many PC manufacturers provide security tools to their customers. In addition, Ofcom is working with Government and industry to help consumers take advantage of the protections such tools provide. Aspects of this work are laid out below.

BSI Standard for Content Control Software

In partnership with the Home Office we have developed a British Standards Institute (BSI) standard for Internet content control software. The standard was announced by the Home Secretary, The Rt. Hon Dr John Reid MP, in December 2006 and the first kite marks based on the standard are due to be awarded later this year.

The Standard, detailing requirements for products, services, tools and other systems aims to allow UK adult Internet users easily to control children's access to inappropriate Internet-based content and services. Products meeting the requirements of the specification will be entitled to display a kite mark on promotional materials and packaging to help consumers identify products which are both effective and easy to use.

Ofcom co-funded this project in support of self-regulation of the Internet, to help consumers to control the content and services they access over the Internet. The overall purpose of the kite mark is to encourage the development of tools that:

— help parents to monitor the activities their children are involved in online;

— help parents enforce limits on their children's computer usage;

— help children avoid accidentally or inadvertently accessing harmful and/or inappropriate content.

By purchasing a kite marked product, parents will have confidence in their ability to:

— install and configure the access control system without needing to be expert or have any specialist technical knowledge;

— protect their children online;

— allow access to suitable Internet-based content and services;

— allow communication with suitable Internet users;

— access suitable system support should they encounter problems with installing, configuring, maintaining or using the access control system.

A sub-group of the Home Office Taskforce has been convened to encourage services to seek accreditation, encourage services to improve child protection and to encourage take-up of the software by parents, through both awareness and other means, including pre-loading. The role of the subgroup will also include ensuring there is a process for review and updating the BSI standard if it proves effective. We expect the Kite marked products will be fully available in the shops in the summer.

Discussions between Ofcom, Home Office and BSI have begun to co-ordinate promotional activity surrounding the award of the first kite mark.

Home Office Task Force

The Home Office Task Force for Child Protection on the Internet aims to make the UK the best and safest place in the world for children to use the Internet, and to help protect children the world over from abuse fuelled by criminal misuse of new technologies.

The following have been created to help keep children safe on the Internet:

— "Good Practice Guidance for the Moderation of Interactive Services for Children"[17];

— "Good Practice Guidance for Search Service Providers and Advice to the Public on How to Search Safely"[18];

— "Guidance for Using Real Life Examples Involving Children or Young People"[19];

— "thinkuknow.co.uk"[20] a website for young people full of information about staying safe online;

— "Good Practice Models and Guidance for the Industry"[21], guidance on chat rooms, instant messaging and web-based services that encourages clear safety messages and advice, and user-friendly ways of reporting abuse.

As well as attending meetings the Task Force, Ofcom contribute to the work of Sub Groups F (Child Protection Measures), G (Awareness) and the newly established International Co-operation subgroup.

— Sub Group F—A working group has been looking at the safety issues for children caused by social networking sites and is close to finalising a good practice guidance document for both users and providers of such sites in the UK.

— Sub Group G—There was further activity from the Home Office marketing campaign between September to November 2006 to support the roll-out of the Centre for Exploitation and Online Protection's (CEOP) thinkuknow schools programme. The online adverts have been particularly successful, and have been seen by over 5.5 million unique visitors. There are 2.9 million 11 to 14 year olds online. CEOP's education programme, entitled thinkuknow, was rolled out to Police Schools Liaison Officers and teachers beginning in September 2006. Thinkuknow is primarily aimed at secondary school children, aged 11 to 14.

— A new International Co-operation Sub Group has been established and Ofcom contribute to its work. This new group met for the first time on 5 December 2006, and discussed the group's aims, objectives, work plan and membership.

[17] http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/moderation-document- final.pdf
[18] http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/search-and-advice- public.pdf
[19] http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/RealLifeExamples.pdf
[20] http://www.thinkuknow.co.uk/
[21] http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/ho—model.pdf

Under Section 14 of the Act, Ofcom is obliged to conduct consumer research on a range of issues, including into the experiences of consumers in the markets for electronic communications services. What research has Ofcom conducted or commissioned, and what uses are the results of this research being put to?

Ofcom and Media Literacy

Ofcom's definition of media literacy, developed after formal consultation with stakeholders, is 'the ability to access, understand and create communications in a variety of contexts'. It is through its Media Literacy work programme that Ofcom is addressing the specific question raised by the Committee.

Research: Media Literacy Audit

In order to gain an initial picture of the extent of media literacy across the UK, Ofcom commissioned an audit of how UK adults and children gain access to, understand and create communications, with a particular focus on electronic communications. In this context, access has a much wider definition than take-up or accessibility issues: it includes understanding of what each platform and device is capable of and how to use its functions; while understanding relates to how content (such as television and radio programmes, Internet websites, or mobile video and text services) is created, funded and regulated.

Some of the elements of this audit—such as attitudes towards the provision of news, or knowledge of content regulation—apply to traditional analogue television and radio as well as their newer digital counterparts. But for the most part, this audit focuses on the four main digital media platforms—not only digital television and digital radio, but also the Internet and mobile phones—as these are the ones where there is most divergence between different groups within the UK in terms of understanding, take-up and usage.

The key objectives of the audit were:

— To provide a rich picture of the different elements of media literacy across the key platforms of TV, radio, the Internet and mobile phones (including some comparisons with other media such as the press and computer games);

— To understand the extent to which there are relationships between the elements of media literacy—for example, is the level of an individual's competence in using the features available on a given platform related to how long they have owned the device and how often they use it? Are levels of concern about the platform related to ownership or usage levels?

— To understand the extent to which there are relationships between the platforms—does interest in, or knowledge and usage of one platform impact upon interest in, or knowledge and usage of another?

The findings of the Media Literacy Audit were published as a series of reports. They are:

— Report on adult media literacy;

— Report on media literacy amongst children;

— Report on media literacy in the nations and regions;

— Report on media literacy of disabled people;

— Report on media literacy amongst older people;

— Report on media literacy amongst adults from minority ethnic groups.

The media Literacy reports are available on the Ofcom website.[22]

Research: The consumer experience of telecoms, Internet and broadcasting services

In November 2006, Ofcom published research which evaluated the experience of UK consumers in telecoms, broadcasting and Internet markets. The research, entitled "The Consumer Experience", highlighted many benefits from increased competition and new technologies, such as falling prices, increased customer satisfaction and a greater range of services. However, it also revealed concerns over the growing potential for consumer harm as communications markets become more complex. The following is a summary of the research's main findings;

Access:

— fixed-line, 2G mobile, digital television and broadband Internet services are available to between 95%-100% of the UK population;

— there has been a 55% growth in Internet users that have taken up broadband in the last 18 months;

[22] http://www.ofcom.org.uk/advice/media—literacy/medlitpub/medlitpubrss/

— only 25% of low income earners have Internet access at home, compared with 88% of high earners;

Consumer empowerment:

— Between 84% and 95% of those who have switched communications provider said it had been easy to switch;

— Only 1 in 5 Internet users have ever switched provider, though more than half have changed their tariff or package;

Consumer protection:

— More than half of all complaints received by Ofcom in Q2 2006 were related to "tag on line", a problem encountered by an increasing amount of broadband subscribers;

— 61% of Internet users are concerned about issues such as paedophiles online, Internet security and offensive content.

What is Ofcom doing to develop public understanding of safe and secure behaviour online?

Promoting media literacy and enabling consumers to make informed choices (extract from Ofcom's Annual Plan 2007–08):

> "In 2007–08 Ofcom will place a much greater emphasis on media literacy, and on consumers' ability to make informed choices and obtain value for money. Taken together, these two areas will lead to people having improved communication capability.
>
> By communication capability we mean the skills, knowledge and understanding that citizens and consumers need to benefit from communications services—to access and engage with content, be able to use communications services confidently and get the best deal in the marketplace.
>
> We recognise that communication capability is dependent on having access to services that are easy to use. Ofcom also has a role in promoting access and inclusion.
>
> During 2007–08 our work to promote media literacy will include raising people's awareness of, for example:
>
> — how to use tools, such as web browsers and electronic programme guides, in order to navigate safely and effectively; and
>
> — how to manage audio and visual content using information, such as content labelling and trust marks, and tools, such as parental controls, Internet filtering and firewalls.
>
> We will also seek to improve people's understanding of: editorial and commercial agendas; the difference between reportage and advocacy; and the context in which content is supplied."

Detail from this year's annual report of activity to DCMS:

> Ofcom's Media Literacy programme is funded in part by a direct grant from DCMS, as opposed to the industry levies which provide the majority of its revenue. As part of its relationship with DCMS, Ofcom provides an annual report of activity, which is summarised below:
>
> — BSI Kite Mark (as above);
>
> — Safer Internet Day: Almost 40 countries took part in the fourth edition of Safer Internet Day (SID) which this year took place on 6 February. The campaign is organised by European Schoolnet, coordinator of Insafe, the European safer Internet network (www.saferInternet.org). Viviane Reding, EU Commissioner for the Information Society and Media is once again patron of Safer Internet Day. In the UK the event was organised by Internet Safety Content Agent (ISCA) Project run by the Cyberspace Research Unit, and Ofcom supported the event and contributed to a panel at a half day conference in London. The event focussed on the theme of 'crossing borders' and included speakers from Ofcom, UCLAN, CEOP, charities, government, education and industry, including Vodafone and Microsoft;
>
> — BECTA: Ofcom is represented on Becta's Safe Use of the Internet Policy Group. Last year the group published 'Safeguarding children in a digital world: Developing a strategic approach to e-safety'. This was presented to the Becta Board, DfES ministers and the Home Office for comment. Ofcom has hosted meetings of the group this year to ensure a co-ordinated approach between the major stakeholders;
>
> — Silver Surfers' Week 2006: In the run up to Silver Surfers' Week 2006 Ofcom in partnership with Digital Unite delivered training to volunteers recruited by event organisers to assist in the delivery of Silver Surfer sessions. By receiving training in teaching techniques and in the use of

resources prepared for events these volunteers were equipped with the necessary skills to deliver on-going training during and beyond Silver Surfers' Week;

— Silver Surfers' Day 2007: Ofcom has begun work with Digital Unite on the development of Silver Surfers' Day 2007. Silver Surfers' Day is the only established media literacy campaign focused entirely on those over 50. Media literacy is becoming increasingly important as digital exclusion is proven to be a core indicator of social exclusion. Older people, who have less opportunity to learn these skills at work or socially, need extra help to acquire them. SSD works by soliciting and empowering hundreds of agencies, public and private, to deliver 'Silver Surfer events' through which they are able to engage with tens of thousands of individuals at a local level and on a national scale.

— Website: The media literacy section includes relevant Ofcom publications, details of forthcoming media literacy events and reports from past activity as well as links to a wide range of external media literacy resources including guides on the safe use of the Internet. It is regularly updated as and when new resources are available;

— eBulletin: Four issues of the Ofcom media literacy bulletin[23] were published in June, September, December and February 2006–07. The bulletin keeps stakeholders informed of developments across the field of media literacy.

Ofcom's enforcement relationship with the Information Commissioner's Office

Areas of common enforcement responsibility

Ofcom and the Information Commissioner's Office (ICO) have discrete and concurrent powers to enforce the Privacy and Electronic Communications Regulations (PECR). The Regulations include the use of automated calling systems, the transmission of recorded messages that contain direct marketing material and compliance with the Telephone and Fax Preference Services.

Enforcement powers

The ICO has primary responsibility for enforcing PECR using its enforcement powers under Part V and Schedules 6 and 9 of the Data Protection Act 1998. Ofcom also has discrete enforcement powers under the Persistent Misuse provisions (ss 128-130) of the Communications Act 2003.[24] Additionally, both Ofcom and the ICO share concurrent powers as Designated Enforcers of PECR under Part 8 of the Enterprise Act 2002.

Enforcement principles and how we decide which regulator takes action

Given our concurrent powers, we have agreed how we will work together in enforcing PECR—we intend to publish a letter of understanding shortly, which sets out the basis of our collaboration.

The following non-exhaustive principles inform our enforcement action in general and which organisation is best placed to investigate issues of suspected non compliance in particular:

General principles:

— Efficiency: Enforcement needs to be quick and effective and should send out a signal that we consider certain behaviour to be unacceptable;

— Co-operation: It is important to work together closely and act in a joined-up way, to ensure that stakeholders have sufficient clarity about our respective roles; and

— Proportionality: Enforcement needs to be proportionate to the risk.

Deciding which regulator takes action

— Special interest: There are areas where Ofcom or the ICO will have specialist experience and might generally be expected to take the lead. Examples might include where the issue of privacy is foremost and the ICO would be expected to take the lead. In contrast, if an investigation would benefit from technical knowledge of the communications sector, Ofcom might be best placed to take action;

[23] http://www.ofcom.org.uk/advice/media—literacy/medlitpub/bulletins/

[24] Ofcom can take action under the Persistent Misuse provisions where it has reasonable grounds for believing that a person has persistently misused an electronic communications network or service in any way that causes—or is likely to cause—unnecessary annoyance, inconvenience or anxiety.

— Clarity: We consider whether the issue raises a particularly novel question (for example, the meaning of a definition in the Regulations or the need to clarify whether a particular practice is permissible or not) which could have bearing on the legal instrument adopted; and

— Resources: We take into account the resources available to our respective organisations at any particular time.

We believe that such an understanding supports appropriate enforcement, providing clarity on the roles of the two organisations and playing to the expertise of both.

Day to day liaison

Ofcom and the ICO keep each other informed on a regular basis about suspected non-compliant behaviour that is causing concern. In addition to informal contact, we also meet at quarterly intervals to discuss enforcement activity.

Recent enforcement activity

The ICO recently undertook enforcement action in relation to compliance with the Telephone Preference Service.[25]

Ofcom also recently imposed a financial penalty of £10,000 on 1RT under section 130 of the Communications Act 2003 (penalties for the persistent misuse of a communications network or service) in relation to their sending faxes containing marketing material to telephone numbers registered with the Fax Preference Service without consent.[26]

Is Ofcom acting on potential security network breaches?

One of the key points about IP technology is it is increasingly available to the end user to determine what their own level of security should be because it allows greater specification at the application rather than transmission layer. It would be particularly expensive to expect Communications Providers (CPs) to provide a very high level of network security which in all but a very few instances would not be called upon. In these instances as they would most probably be criminal in intent, they would properly be dealt with under existing criminal law. From Ofcom's point of view the General Authorisation Regime, introduced in July 2003 to replace the system of telecommunications licences, regulates how Communications Providers (CPs) should provide Electronic Communications Services (ECS) and/or Electronic Communications Networks (ECN).

Under this regime there are a number of General Conditions (GC) which providers of ECS/ECN must abide by. The majority of these GCs cover consumer protection in terms of their contractual relationship with the CP and their access to certain services, however two GCs in particular also deal with technical aspects. GC2 requires a CP to conform with appropriate standards for the purpose of ensuring the viability of interconnection and end-to-end interoperability. GC3 requires a CP who provides a Public Telephone Network (PTN) or Publicly Available Telephone Services (PATS) to ensure the proper and effective functioning of the network. However, neither of these GCs specifically require a CP to protect the confidentiality of the information it carries across its ECS or ECN, nor to secure the network against external interference. Nevertheless, it is clearly commercial good practice to do so as the risk to any CP's business of not doing so is obviously very high through a loss of confidence in it as a responsible CP.

Ofcom would be concerned if any CP, particularly a provider of a PTN or PATS, took an irresponsible approach to maintaining the integrity of its customers' data and the network but ultimately the choice of the level of security to apply to one's data is a choice for the end user which is why some consumers choose to apply their own security at the application layer rather than relying on the network to maintain security and integrity. Some CPs may also offer products which provide contractual security and/or integrity guarantees.

Most CPs, for the reasons stated above, will take significant steps to protect their network against intrusion but there is clearly a risk of interference which with such a widely distributed asset as an ECN is very difficult to completely mitigate. It is not possible to detect all attempts to interfere with the network and there is always a risk that an intruder could go undetected and gain access to user data, eg by tapping the line between the end user and the exchange, and it would be unreasonable for a CP to regularly check the entirety of all of its

[25] http://www.ico.gov.uk/upload/documents/pressreleases/2006/en—6—dec—06.pdf

[26] www.ofcom.org.uk/bulletins/comp—bull—index/comp—bull—ccases/closed—all/cw—891

physical and software assets for unauthorised access. Indeed such monitoring would be extremely costly, the cost of which would need to be recovered from consumers. It is therefore sensible for consumers never to assume that the network is entirely secure and to implement their own security measures.

Regulation of Voice over IP services (VoIP)

In March 2007, Ofcom published a new regulatory code for Voice over Internet Protocol (VoIP) service providers to ensure that consumers have access to important information about the capabilities of their service.

Following public consultation in 2006, Ofcom has decided to put in place measures to ensure that consumers have access to information which helps them make informed purchasing decisions. The new code of practice requires VoIP providers to make clear:

— whether or not the service includes access to emergency services;
— the extent to which the service depends on the user's home power supply;
— whether directory assistance, directory listings, access to the operator or the itemisation of calls are available; and
— whether consumers will be able to keep their telephone number if they choose to switch providers at a later date.

If consumers choose to take up a service that does not offer access to emergency services or which depends on an external power supply, the code also requires VoIP providers to:

— secure the customer's positive acknowledgement of this at point of sale (by ticking a box, for example);
— label the capability of the service, either in the form of a physical label for equipment or via information on the computer screen; and
— play an announcement each time a call to emergency services is attempted, reminding the caller that access is unavailable.

As usage in the UK continues to grow, and the market develops further, Ofcom will continue to review and develop its approach to regulation to ensure that consumers gain the full benefits of VoIP services.

A number of respondents to Ofcom's consultation expressed concern that a lack of access to emergency services via VoIP services might result in consumer detriment. For that reason, Ofcom intends to consult later this year on whether, and if so how, certain VoIP services might be required to offer access to emergency services.

11 April 2007

WEDNESDAY 25 APRIL 2007

Present	Broers, L (Chairman)	Mitchell, L
	Errol, E	O'Neill of Clackmannan L
	Harris of Haringey, L	Sharp of Guildford, B
	Hilton of Eggardon, B	Paul, L
	Howie of Troon, L	

Examination of Witnesses

Witnesses: COMMANDER SUE WILKINSON, Metropolitan Police, MR BILL HUGHES, Director General and MS SHARON LEMON, Deputy Director, Serious Organised Crime Agency, examined.

Q1032 ***Chairman:*** Thank you very much for coming to give evidence to us. This is the House of Lords Select Committee for Science and Technology and this is in fact our final evidence session, at least as presently planned for this inquiry, which we have been conducting for several months. We very much appreciate you coming to talk to us. Welcome to members of the press and the public who are here. I assume you have picked up the documents that tell you what the Committee's mission is here. Perhaps we could start with our witnesses introducing themselves please.

Ms Lemon: My name is Sharon Lemon. I am the Deputy Director of the Serious and Organised Crime Agency and the Head of e-Crime. Formerly I was the Head of the National High Tech Crime Unit and before that the Head of the Paedophile On-Line Investigation Team. On the first of April last year I handed the ACPO lead to Commander Wilkinson, SOCA not being a law enforcement agency. I chair the National e-Crime Strategy Group and chair the steering group for Get Safe On-Line.

Mr Hughes: I am Bill Hughes. I am the Director General of the Serious Organised Crime Agency which actually is a law enforcement agency, not a police agency. Prior to that, I was the Director General of the National Crime Squad. The National Crime Squad and the National Criminal Intelligence Service are part of Customs and Excise, as it then was, part of the Immigration Service and were brought into SOCA at the beginning of April 2006 so we have just had our first anniversary of working.

Commander Wilkinson: I am Sue Wilkinson; I am a commander in the Metropolitan Police. I have the lead for e-crime in the Metropolitan Police but also last April I took over the ACPO national lead within ACPO forces for e-crime. I also, within the Metropolitan Police, have responsibility for fraud and economic crime et cetera which is closely allied to e-crime. I chair the Internet Crime Forum and I run the ACPO working group on e-crime.

Q1033 ***Chairman:*** Thank you. Is there anything you would like to say in an opening statement?

Mr Hughes: No, I do not think so except perhaps to say that when the National Crime Squad was abolished and SOCA started there was a change over obviously from what was a specialist unit within the National Crime Squad which was the National High Tech Crime Unit and that has moved into a different approach within SOCA. Some people would see that that showed a lack of interest in e-crime; the reverse is the case. SOCA went to a situation where we have a unit now called e-Crime which Sharon heads which devotes itself to that type of criminality. The issues around paedophilia on-line went into a separate unit called CEOP combating child exploitation and on-line protection which is an affiliated unit to SOCA. We marshalled our resources in a better way in order to be able to deal with e-crime issues and at the same time working with the Metropolitan Police and ACPO have started to look at ways in which we can make sure that we spread that right across the piece in a continuum rather than simply having different squads dealing with issues.

Q1034 ***Chairman:*** That leads into my first question which is a very general one which is: is there such a thing as e-crime? What I am really leading to is whether e-crime should be formally defined and, if so, how should we go about that?

Ms Lemon: We have defined it as two specific areas. Firstly the type of crime that can now be committed because technology exists which formerly could not be committed; I think that is definitely e-crime because without the technology those crimes could not be committed. More commonplace now is traditional crime moving on-line in the virtual environment, traditional criminals using and exploiting technology; that is traditional crime using technology. That is where we need to mainstream the issues more because I think the problem with policing is that anything involving a computer or the slightest bit of technology is put into a specialist bracket and it is confusing the issue and leaving a smaller number of specialist resources dealing with what is traditional crime. So we have a clear definition; we have type A and type B where we are talking about technology

that enables this crime to exist. Normally traditional crimes, even so, the denial of services attacks, is just current day extortion; phishing is just current day fraud, and then there are traditional crime types. I think there is definitely an e-crime but the biggest part of the issue is that all the crimes that are exploiting technology just make it much easier to commit the crime.

Q1035 ***Chairman:*** Do you think you are now in a position to start gathering statistics and setting targets for yourselves on e-crime?
Ms Lemon: I would not be so bold as to say that we are anywhere near gathering statistics at the moment. We can certainly look at the evolution of e-crime which has been well documented from the people committing the crime just because they could for kudos, to now people exploiting the type of crime because of the revenue that comes with it. There is a very quick scale and reach. We see traditional criminals committing their crime on-line but I do not think I would be so bold as to say that I would be able to give you an estimate of what it looks like in the UK at the moment.

Q1036 ***Chairman:*** Are you trying to move towards a situation where you can gather statistics?
Mr Hughes: If I may answer that question in a different way, that is the point that Sharon has made is that whilst these are often old crimes committed with new techniques, the issue is how do you deal with them. It is not so much a matter of how you record them or how you see them as crimes per se for investigation, it is how best to deal with them. I think that is the issue that we all need to be thinking about now. The way it is done is often because this is a global issue. This is not just happening inside the UK so expecting UK law and enforcement necessarily to pick up on it and to be able to deal with it on its own is not feasible. There need therefore to be global alliances; we need to be able to work with our colleagues in other countries in other parts of the world. There needs to be another way of actually pulling the information together. People simply coming into police stations to report the crimes is going to end up with an uncoordinated approach across the whole of the United Kingdom and outside. What we need are better ways of gathering the data about what is actually happening so that with our colleagues in the private and public sector who are helping with that—we will probably come onto that later—there are ways of building up crime pattern analysis which can help us to attack and deal with what is happening there rather than investigating each individual case one its own. This is very much the way that SOCA is trying to deal with serious organised crime per se and the way that the police service is also picking up on dealing with crime pattern analysis and taking out the root cause rather than addressing the symptoms. This is a classic example where we need to change the way that we work as law enforcement.
Commander Wilkinson: Obviously I am sitting here representing the 43 police forces of England, Wales and Northern Ireland and I would certainly hope that by the end of this session the Committee has clarity around how the 43 police forces of England, Wales and Northern Ireland will work seamlessly with the Serious Organised Crime Agency in tackling what is a crime that is very, very difficult to define geographically and in terms of numbers of victims and geographic location of the crime is almost impossible to really pin down or define. When I took over the national portfolio on e-crime we reassessed the old ACPO definition of what was then high tech crime and we redefined it and made it much simpler. The ACPO definition of e-crime (it may be helpful for you to know it sits comfortably with the SOCA definition) has been agreed as the use of networked computers, telephony or Internet technology to commit or facilitate crime. That is clearly very, very wide indeed. When we are looking at e-crime we have to look at it from being solely an e-crime, if you like—such as a denial of service attack, for example—right the way through to traditional crime such as fraud or kidnap or any other traditional crime during the commission of which technology comes into it, whether it is the use of text messaging or actual money laundering through computers or the use of mobile phones, et cetera. The definition is incredibly wide because it has to be so that we can pull everybody into the fight against e-crime and we can mainstream it. It does also make it incredibly difficult to count the number of so-called e-crimes that have actually taken place.

Q1037 ***Chairman:*** Is there evidence that conventional crime is being displaced by e-crime? Is it apparent to you that you can shift resources now? You do not necessarily need new resources but you need to shift resources and re-train people.
Mr Hughes: There are two issues there. There is clearly evidence that we are seeing serious organised criminals working in an area which is new to them. As always these are entrepreneurs who go where the rewards are high and the risks are low. They are looking at ways in which they can move into new areas of criminality. In terms of law enforcement, we also have to look at ways in which we train and restructure ourselves and resource ourselves better. E-crime is a classic example. What we need from Sharon is very much a specialist area of enforcement understanding, but if you just parcel this off into separate squads or separate units within law enforcement then you are missing the trick. The trick we have to make sure people realise is that this is

going to be the way of the future. We have to mainstream it so that the detectives, investigators or law enforcement agencies are starting to think about how this impacts upon the type of investigations they are dealing with. It is as simple as, for example, every time we deal with serious organised crime there will be a laptop, a PDA, a telephone or some very complex piece of kit and we need to have the understanding of how this can be used and, more importantly, how evidence can be gained from that technology in order to prosecute our cases or to gather the knowledge and information we need to be able to attack the source.

Commander Wilkinson: I totally echo that. I think from the point of view of the police forces we need to raise the level of awareness, understanding and capability across all officers; uniformed constables for example and detectives will need to have a higher level of capability and skill so that everybody has some awareness and capability in terms of investigating e-crime and there are certain types of e-crime that are so specialist that there will need to be specialist units to deal with those. I would echo entirely the point that it needs to be mainstreamed because this is the way we live now and it is a developing way that we live now and so it is important not to try to shift everything into specialist units but to raise the level of awareness and capability right the way across the board.

Q1038 ***Lord Mitchell:*** Perhaps it is appropriate that as we speak the Serious Crime Bill is going through our House and we may have to go and vote a few times on it. One of the issues we have looked at quite a bit in our deliberations is whether the legal framework for investigating and prosecuting e-crime is sufficient. Do you feel it is sufficient and are there any gaps that need to be plugged?

Ms Lemon: As far as I am concerned in the UK I do not think there are any significant gaps. I would not want to make legislation overly complex—and this goes back to the mainstreaming part—as long as recognition is made in forthcoming legislation of the need to include technology and it is a neutral bit of legislation that would incorporate what we need to achieve. Where it is difficult for us is in the international space where legislation in different countries can cause problems. The current procedures for sharing information and intelligence can be extremely sluggish and sometimes we work despite those arrangements, so that would be a problem I would like to raise.

Commander Wilkinson: I think for me the Computer Misuse Act, the latest Fraud Act and existing legislation is proving entirely adequate to incorporate the issue of e-crime into it in terms of investigation, evidence gathering and prosecution. However, the issue of the international nature of e-crime is probably our biggest challenge and investigations can fall down because of the fact that legislation does not really cover the international challenge. We cannot prosecute offences that are committed abroad, for example, and criminals can exploit that by originating the offence abroad.

Mr Hughes: If I may add just one further point, that is the question about the prosecution as well. Of course much of this revolves around how we present cases in court and the abilities of the courts in the UK particularly to receive particularly complex information from IT investigations or the way it is presented is difficult. This is no fault of the courts; this is simply that we are living in a fast moving world and perhaps one of the things we should be thinking about is how better we can present the case in court so that judges and juries better understand exactly what is being presented there. In the same way that you have a technological advisor here it may be useful to do the same in some of the courts when we are dealing with some of these cases.

Q1039 ***Lord Mitchell:*** On that sort of related issue, would it be feasible for a computer used to commit a crime to be brought out in court and sentencing in a manner in some ways analogous to the aggravating factors of bringing out a gun for other types of crime?

Mr Hughes: That is an interesting question. You referred just now to the Serious Crime Bill that is going through your House at the moment, and there may be some prevention orders in there that we might like to think about as examples of what we could do with those who had such criminality. There is no doubt we could use that effectively.

Q1040 ***Lord Mitchell:*** We have already touched on the issue of whether an e-crime is a traditional crime just done in a different way, but nevertheless the economics of the crime—which I think you also mentioned and which is the mass nature of it (we see this in large scale phishing attacks which can yield a high profit for relatively low investment)—does this actually transfer it into a different type of crime?

Mr Hughes: Again, as both of my colleagues have said, I think the present legislation is right. What we would look for particularly is that perhaps this is an area which could be reflected in the sentencing, depending on the aggravation factor. If I give one example, we are investigating at the present time a fraud which many people in this room will probably have known about for a long time, which is when you receive a card telling you that you have won the lottery despite never having bought a ticket. If you pay a certain administrative charge and so on and so forth they will get you the winnings. This is a clear scam and it is operated often outside the jurisdiction. It is small scale but when you pull it together these

can involve millions of pounds being taken from people. More importantly they are targeting vulnerable people because once you respond they put you on a sucker list and then they go back to you and back to you and back to you. This targets the more vulnerable in society. I would want to see, if there were a way of explaining and bringing that to the fore in a court case, that that should be reflected in the sentencing because of the aggravation factor of what is going on.

Q1041 ***Lord Harris of Haringey:*** Following up on that in terms of the exacerbating factor, you have just given us an example of the sucker list and so on but we have also received evidence about the vulnerability of young people and new forms of bullying which are e-related. The nature of this is that the message or the crime is committed through something which is sitting in people's homes frequently. That is therefore a different sort of intrusion from when you might be more on your guard when you are going about your daily life outside. Do you think that that could be built in as some sort of exacerbating factor in terms of crime, that because of the computer sitting in people's homes—in their living rooms or their bedrooms or wherever—that this is something which makes the crime worse and should be taken into account in terms of sentencing or in terms of recording?
Ms Lemon: I certainly think that in terms of bullying the effects could be far more damaging because the attacks could be so much quicker and more intense. If you are getting bullied by a text message of SMS or IMs it is there constantly, whereas if it is a physical bullying (which is equally bad) you have to actually engage with the person on the occasion you see them. Certainly it is an aggravating factor because it is then invading the whole of your life.
Mr Hughes: I think the point you raise, Lord Harris, is a very important one. This takes me back to when we started doing drug investigations and often you would find courts who were not familiar with the effects of a particular drug or how large or what the significance of the sort of seizure was that had been made by police or customs officers and how much money and how much damage that could cause. We may actually be in that same type of environment that you are describing now where everybody has a laptop or desktop in their home and it is just seen as a piece of equipment in the house like a toaster or a kettle, but it is not because of the points you make; it can be used in another way. It may be that we need to point this out particularly with young children being bullied in this way either by SMS messages or e-mails that have been sent to them or in some cases where they have sent them to other people themselves. This is the point I was making just now, how do you present this in a court case where you can realise the aggravating factors and the damage that this can cause. This again may be something we want to look at in terms of prevention orders. It may be around not having access to such technology or not being allowed to use it in certain areas. I have to say as well that the issue here again is about education, making sure that people understand that having a desktop in your house there are certain things you need to be aware of. There are many beneficial aspects of having it, but there are dangers to it also. If I may say so, that is one of the reasons why Jim Gamble with CEOP is making such a strong case around protecting children on the net and the Virtual Global Taskforce, police officers patrolling the net through the use of that Virtual Global Taskforce to try to reinforce that message that this can be used for ulterior motives.

Q1042 ***Lord Harris of Haringey:*** The Home Secretary I think has recently announced that he wants crimes where there is the use of a knife for there to be a separate recording category so that the fact that the knife has been used is recorded for data purposes. Would you see some value in respect of all crime in there being some recording where it is e-enabled simply to give some sort of indication of the problem of the scale and the issues?
Mr Hughes: I think there would be benefit in that. I also think, from the point of view of criminal intelligence again, you are looking at recording knowledge about how a crime was committed, building up a picture, crime pattern analysis, the knowledge and MOs of individuals it would be useful, but that is me talking like a cop now. From the point of view of protection of communities, I think it would be useful to do that. Again it gives you the point that was made earlier on about picking up targets. At the moment what is actually happening in terms of e-related crime is a little bit in the dark. We do not know too much about the numbers involved and it would help us to pick up on quantifying what the actual problem is.
Commander Wilkinson: The Metropolitan Police is flagging crimes which have an e-ingredient and it is giving us some idea perhaps of the proportion of crimes that are actually reported that have an e-element. However, it is really complex because is the use of a telephone during the commission of a crime an e-crime, right the way through to the crime which is wholly facilitated or commissioned on the Internet? It is a difficult question. I think we should aim towards that eventually, but as the world modernises and moves on you are going to end up with the vast majority of crime actually being shown as having an e-ingredient. In the Met we do actually record offences and we code against whether a hacking virus has been used in the course of the commission of the crime, whether a computer has been used to facilitate the offence (which could be to any degree really) and

other offences where the Internet is being used. We do not currently count any crime that is committed using a mobile phone, for example. Certainly this is something which I shall be looking at. You are probably aware that I have recently received endorsement from the Chief Constable's Council to go ahead with setting up a police e-crime unit that will actually pull together policy, practice, standards and training across the whole of the 43 police forces and this is one of the key initial aims of this unit, to try to standardise recording, reporting and statistical analysis.

Q1043 ***Earl of Errol:*** You made the point that some of these things are outside your jurisdiction. Surely if the crime is perpetrated against a UK citizen in the UK the fact that the initiator of the crime happens to be resident outside the UK at the time is still in your jurisdiction, in which case could you grab them, like the Americans do, using a European arrest warrant?
Mr Hughes: The European arrest warrant is there to be used; it has potential. That is provided it is within the European jurisdiction, a lot of people we are dealing with are not.

Q1044 ***Earl of Errol:*** If the victim is in the UK does it then fall within your jurisdiction?
Mr Hughes: It depends on the strict definition of the offence, where it is perpetrated or where it is actually put into effect. If it is done via an e-mail or something like that then you have to prove where it has originated from of course.

Q1045 ***Earl of Errol:*** The victim is in this country.
Mr Hughes: That is true.

Q1046 ***Earl of Errol:*** He has parted with money in this country.
Mr Hughes: I accept that. We could probably spend several hours debating the legal aspects of all this.

Q1047 ***Earl of Errol:*** So we are going to have to look at the law on this.
Mr Hughes: I think the law is quite robust around this. The real point is that a lot of the people we are dealing with are outside the European jurisdiction as well and that is why we are putting global alliances into place so they can be dealt with in their country of origin.

Q1048 ***Baroness Sharp of Guildford:*** To what extent do you think e-crime in the UK is actually increasing, and in particular given the caveats you have already announced about statistics, how far do you think the data based on e-crime is reliable and how far it is not?
Ms Lemon: Definitely evidence of traditional off-line crime now going on-line because of the scale and reach and the instant contact around the world. We are forming very successful partnerships in the UK to share information intelligence around e-crime which I think is extremely promising. We have formed the National e-Crime Strategic Group which is going forward with different agencies in the UK to share intelligence and information. Bill referred to the global alliances we have where we are also sharing information about threats. I think we are getting a much more comprehensive picture but with a full admission that we have a long way to go.

Q1049 ***Baroness Sharp of Guildford:*** Given the comprehensive picture do you think it is going up or down?
Ms Lemon: I think certain areas are going up. The money-motivated crimes are on the rise; the "I can open the Pentagon crimes because I'm clever" are on the decrease. Money-motivated crimes are on the up.

Q1050 ***Baroness Sharp of Guildford:*** In Get Safe Online, the survey where they announced the results last October, what they found was that people feared on-line crime much more than they feared mugging and burglary. Would you agree with that?
Ms Lemon: Those were certainly the findings and my plea from this group would be about raising levels of awareness with realistic information for consumers, businesses and home users because unfortunately there is not a systematic way of informing consumers and we get dramatic headlines which do scare people when they do not know how to deal with an e-mail. I think there is a remedy through Get Safe Online perhaps promoting that and developing it. I think people need pragmatic, realistic advice to encourage them to use the on-line environment, which is what we would recommend.

Q1051 ***Baroness Sharp of Guildford:*** How much of the e-crime experienced by UK citizens is actually committed by criminals based in this country and how much comes from abroad? Do you have any feel for that?
Ms Lemon: I speak for the Serious Organised Crime Agency. Most of our offenders in the level three crime, causing harm to the UK and its citizens, are by people outside of the UK.
Commander Wilkinson: We do not have accurate statistics but that does appear to be the case.
Mr Hughes: Just to pick up on some of those areas, again it is back to becoming aware of how this crime is actually happening because, as you will know, there is a lot of hyperbole in the press, media and elsewhere, a lot of scare stories; sometimes they are very valuable but we have to be careful to sort out the wheat from the chaff on this one. That is why one of the things we are trying to do—and Sue's unit will be doing as well—is working with our colleagues in other sectors. For example, banks and financial

institutions that can help us to get a picture round what is actually happening. You have talked of the fear of the crime, people have a fear of phishing attacks. They need to be on their guard but we do not need to slow everything down and stop e-commerce. We have to get some accurate picture out of that. If you read some media you will think that everybody is subject to a phishing attack but it is not that many numbers but equally when they are then it can cause serious damage. What we need is for the banks to give us some accurate picture, and they are being very helpful on this. Now of course we have moved on because the approach that we are taking where they are not fearing to tell us that they have been subject to this where in the past for competitive reasons they kept things quiet so we did not really become aware, now we have ways in to talk with them in confidence. Sharon and her team and the police forces now have ways to pick up the picture without exposing them to the risks of losing customers because they have had this attack. Unless we do that, unless we have that confidence, then we will not get an accurate picture of what is really happening.

Q1052 ***Baroness Hilton of Eggardon:*** To pursue the matter of getting an accurate picture, when we visited the FBI in the States we heard about the IC3 network which obviously would be very resource intensive, but it would help you to analyse patterns and so on. Do you think we should have something which is much more publicly known about the ways of reporting e-crime?
Ms Lemon: The IC3 essentially is very good for analysis and intelligence but it is not the single reporting centre in the US; it is an option. A third of their reports come from out of the US so that gives a few pieces of the puzzle and my comment would be that if we are going to have something let us have all the pieces of the puzzle.
Commander Wilkinson: We did visit the IC3 centre as part of our preparation for setting up the new police unit and we will definitely take some best practice from there. I think we have a lot to learn from it. However, I think that there is a new issue emerging in the UK around the new strategic fraud authority and the new potential national fraud reporting centre that is currently being scoped by the City of London Police. Clearly so much of e-crime relates into fraud that actually the last thing we need to do now is start talking about a national e-crime reporting centre which would eat up a lot of money unnecessarily and will duplicate. I am currently talking with the Commissioner and his staff and the City of London Police to work out how any potential national fraud reporting centre can merge with e-crime reporting and build into the fraud reporting centre the extra types of crime that may be reported that are not specifically fraud. That is something we need to look at immediately in terms of the planning that the City of London are going through.

Q1053 ***Baroness Hilton of Eggardon:*** Do you see that as an ACPO responsibility rather than a SOCA responsibility?
Commander Wilkinson: I would, I think, yes, because we are the public face of law enforcement and policing in this country. Given the fact that the City of London are already scoping this particular issue we need to work closely with them to see how we can merge e-crime reporting in with it.
Mr Hughes: Just to pick up on that, we are not in competition here; we are in competition with the bad guys. That sounds like a statement of the obvious but it has not always been that way and you know that very well indeed. The benefit of SOCA is that we are part of a continuum of law enforcement in this country and not an "instead of" which you will see from the cooperation and the collaboration here. The other point I would make as well is that the point you make about the ability of individuals to be able to report this to a law enforcement agency whomsoever, we are not complacent about that. We still have some way to go on getting this right. That is why we are working on this strategic grouping to get all of these different agencies who are beavering away in different areas pulling that work together and they can assure the individual, when they have been the victim of a crime, of a way of reporting it. This is what Sue was talking about, that mainstreaming. If you go into one police station in one of 43 police forces this is not going to be the best way of coordinating that response back to us. It will take time and the problem with the crime we are dealing with here is that it is very fast, very dynamic and they move quickly so we have to be able to do the same. We need to find ways to reassure individuals when they do report that their inquiry is being dealt with, to find ways of dealing with it at source rather than simply starting with the investigation side. If you like, that is one of the changes in law enforcement that we are trying to push through, both of us.

Q1054 ***Chairman:*** Continuing on with the theme of who has responsibility, who is responsible for investigating level two e-crime which appears to fall outside the responsibility of both individual police forces and of SOCA?
Commander Wilkinson: The Metropolitan Police Service has a computer crime unit and does take on those types of investigations that fall outside of those two remits. Certainly the new national unit or the new ACPO police e-crime unit that we now have the go ahead for would be the repository for such reports and would certainly assess such reports and decide how they should be investigated any by whom. The Metropolitan Police is currently carrying that

responsibility; the new unit will be housed within the Metropolitan Police in any case. The point that is important to make is that Sharon and I are currently working on putting together a protocol whereby the nature of e-crime is such that any small local report can turn out to be the end product of a multi-national crime issue. Therefore it is very important that the protocol between the 43 police forces of SOCA works well so that we can work out exactly who is best placed to investigate. Often a level two crime is actually a level three crime; it is an international crime. We are working that through at the moment.
Mr Hughes: It is one of the areas that is vital in what we are trying to do with SOCA and the way the police forces work. If we do not understand and have the knowledge around the whole of the problem then we will go at it piecemeal whereas what we need to understand is what is actually happening here? What you are seeing is the end result, as Sue has just said, of something which has started elsewhere and may be happening elsewhere and there is another way of attacking it. If we only focus on the individual case we will only forever be rushing round with sticking plaster whereas we need to be looking at the whole issue. There is a danger when talking about levels one, two and three—we have found this elsewhere on the national intelligence model—people seem to think that crimes fall into nice convenient slots and that the law enforcement response can follow that same route. It does not; it has to be a continuum activity and understanding so that we can address it properly. That is why we are working so closely together so that nothing does fall between the stools.

Q1055 ***Chairman:*** This is an issue that we have focussed on quite a bit. If we look at this from the point of view of the individual in the United States we learned from the Federal Trade Commission that they have tried to generate a standardised form that the 28,000 police stations in the United States can have so that an individual now knows what to do. Presumably one hopes it is then coordinated and that is certainly their aim. If you look at the environment here, we understand that individuals could approach the National High Tech Crime Unit.
Ms Lemon: The National Crime Unit never took reports of crime. We did provide advice on our websites and we did have people answering the phone for general inquiries. That is still the case with the exception of the website.

Q1056 ***Chairman:*** What should the individual do today? We learned from Gareth Griffith, the Head of Trust and Safety for eBay that "When we try to get police engaged, sometimes they say, 'Look, we'd love to help you. If it is not over x threshold'—thousands of pounds, or whatever it is—'we can't help you'." Is this true? The individual who has lost £500—which is important to the individual of course—does not look very large to an enforcement agency but it may be one of a thousand such cases.
Mr Hughes: You have picked up on exactly the issue I was making which is e-Bay, for example, comes straight into us. Banks and financial institutions come straight into us because we have set up this way of picking up the issues so that we are picking up a big picture rather than simply responding to individuals. e-Bay will see where there is a pattern emerging and we can do something about it. You are absolutely right and again we are not being complacent. There needs to be a way for private individuals to be able to report a matter to the police service and that is what Sue and her team are working on doing. This is going to take a little time to put across the country. As I say, the danger with it is that every different police station across the whole of the United Kingdom, getting all that information in and being able to deal with it, there are other ways in which we deal with crime, perhaps in a different way, and that is also what we are looking for. I have no easy answers to that at all; it will take time to develop.

Q1057 ***Chairman:*** Are you definitely assuring us that this feeling that people have, particularly with industry, that the abolition of the National High Tech Crime Unit demonstrated that the police were no longer serious about e-crime; you are saying exactly the opposite, are you?
Mr Hughes: That is not the case. It is one of those things where SOCA is one year old; we have been working through a new agency. We have established through several of our different units—Sharon's is just one—with the Prevention Alerts Unit, the Crime and Techniques and other areas around proceeds of crime, the Suspicious Activity Reporting Database that we have been enhancing since Sir Stephen Lander's report that has helped banks and financial institutions report stuff to us. All of those are ways in which we are going out into what is happening out there to find out the true picture. As I say, there was a lot of bits and pieces written in various media about the National High Tech Crime Unit which, on occasion, bore little link with reality. What we are trying to do is establish something which will actually take forward in a better way the response that we need to have. We are not there yet; we are working on getting it there.
Commander Wilkinson: From the point of view of the 43 police forces, I cannot sit here and assure you with total confidence that if any individual member of the public was to go into any police station in the UK that they would immediately get the level of service they would expect in terms of the person they were reporting the crime to understanding exactly what the problem is. This is one of the tasks that I have really set myself in setting up the new ACPO unit, to

mainstream awareness and a certain level of skill amongst all police officers and police staff so that we can provide a better level of service. However, I am quite robust around this because I think that the nature of e-crime, because it is often geographically very wide and because often there may be many thousands of victims of one particular crime, I cannot—and I will never, I do not think—be able to take the position whereby I will be able to say to any single member of the public that every single e-crime will be investigated. What we need to do is to collate the picture of what is going on and there are a lot of different means already in existence of doing that and through various websites et cetera. We need to get a full picture of the pattern and the nature of the crime in order to tackle it in a very pro-active, preventative way, to stop it happening in the first place. Often the scale of the crime is such that the police service would just fall over if it tried to investigate each of them on an individual basis. It is a different type of crime from that point of view; this is a new type of crime where the technology is allowing a new scale of crime that we cannot deal with in the conventional way.

Q1058 ***Lord Harris of Haringey:*** If a member of the public reports something to the new national unit, if it meets the investigative criteria and it fits into a pattern, then it will be followed up, it will not simply be a tick in the box, is that correct?
Commander Wilkinson: Potentially it would be followed up. There will be investigators for major crime that is causing major threat or major harm at a level two, level three basis for example. I do not have those terms of reference or those criteria clear yet. We have only just got the go ahead for the unit in the first place and that all needs to be worked through and will take some time to work through. I am very conscious that the 43 police forces need to provide a better standardised service in terms of the reporting and the investigation of e-crime.
Chairman: We will have to adjourn for a few minutes now for the division.
The Committee suspended from 4.28pm to 4.36pm for a division in the House.

Q1059 ***Lord Harris of Haringey:*** Could I just follow up about the National Unit? You have told us you have the go-ahead; does that mean the funding is in place?
Commander Wilkinson: It does not mean that funding is in place but we do have a plan. We potentially have a great deal of sponsorship and we are now going to start work on a detailed business case to work out exactly what is likely to be forthcoming. That really is the very next step that we now need to take. I have no doubt that a considerable amount of sponsorship will be forthcoming and I have no doubt it will be enough to set the unit up. It needs to be managed well because this is a law enforcement unit with private industry backing it.

Q1060 ***Lord Harris of Haringey:*** Does the Home Office need to support it to unlock the private sector funding?
Commander Wilkinson: I am going to go back to Vernon Coaker who is the minister concerned with the detailed business case when it is completed.

Q1061 ***Lord Harris of Haringey:*** Do you think it needs the Home Office to give their support and provide some funding to unlock the private sector finance?
Commander Wilkinson: Vernon Coaker has already given his full support of the unit and I need to go back to him with the financial situation and put a business case to him. I have no undertakings currently of government support but I have not actually specifically asked for it yet.

Q1062 ***Lord Harris of Haringey:*** The private sector sponsors are not saying that their support will be conditional on Home Office financial support.
Commander Wilkinson: I have not had that specifically said to me, no.

Q1063 ***Earl of Errol:*** My understanding is that since the Home Office failure to match funds for the Dedicated Card and Plastic Unit the private sector was somewhat more sceptical about Home Office indications that they would jointly fund or match funds for these things in the future.
Commander Wilkinson: I am sure there is some scepticism and clearly there have been some cuts in similar areas recently of existing funding but, as I say, I have spoken to the Home Office minister concerned on two occasions now about the actual unit and he has asked me to go back to see him again once the chief constables have given their endorsement—which they have done—and once the detailed business case is prepared and ready, which it is not yet, we are in the throes of doing that at the moment.

Q1064 ***Earl of Errol:*** My understanding is that the Home Office will not designate e-crime as a separate crime or a separate category as they do not want to muddle the fraud figures and the other forms of crime. If they refuse to recognise it as a separate form of crime or as another means of committing crimes, will that not make it very difficult for them to provide funding for a unit?
Commander Wilkinson: I think it is more a question for me of making sure that the e-crime issue is part of the national strategic assessment and appears in the national policing plan, the national community safety plan. When I have got to that stage—I am working towards that as well—I think by making it

more of a priority in terms of police aims and objectives nationally that is the way to get resources put into it not only from government but also around the country from the various police forces.

Q1065 ***Lord Howie of Troon:*** Last weekend I had occasion to go down to the south coast near Beachy Head to visit my daughter and grandchildren. While I was away my burglar alarm went off. My next door neighbour rang up the police who did not seem to be terribly worried about this. Do you treat e-crime with the same promptness as they do?
Commander Wilkinson: It is very difficult for me to comment on individual cases.

Q1066 ***Lord Howie of Troon:*** They are all individual cases.
Commander Wilkinson: Yes, and I was in the throes of answering that question when the bell went. Because of the scale of e-crime across the board it is impossible for us to individually investigate every single report of it. What we are doing is getting an ever improving intelligence picture around what is happening in terms of trends and types of e-crime that are being committed. We are working in partnership with industry and other law enforcement agencies to cut it off at the root, if you like, and to stop it happening and to get ahead of the game. That is actually, I think, the most effective way we could tackle e-crime. If an e-crime is reported to us that represents a particular amount of threat or harm to any individual or to any critical national infrastructure or whatever then clearly that would immediately be risk assessed as one that needed to be investigated separately.
Lord Howie of Troon: I am very happy with that answer. It turned out to be a false alarm; I do not have anything worth stealing anyway.

Q1067 ***Lord Mitchell:*** The individual reporting this type of crime feels very, very stupid; for the small amounts of money he feels very stupid and will not take any action on it. This is the issue, is it not, they work on the fact that there are millions out there who have small crimes and therefore they do not report it?
Commander Wilkinson: I would hate any member of the public to feel they could not report a crime that concerned them to us. The important thing for people to understand is that each individual e-crime cannot necessarily be individually investigated. Certainly part of my remit with my national hat on is to make sure that people receive a decent quality of service whatever they are reporting to the police. Having said that, there are a lot of other ways that people can draw crime to our attention. There are various websites where people can tell us what has happened in order for us to get a much better intelligence picture about how to prevent it happening in the first place. We need to promote those websites; although they are pretty well promoted already we need to promote them more and to improve accessibility to the websites. By improving that intelligence picture we can tackle all of this much more effectively in the big picture.
Mr Hughes: The analogy of policing has always been the same. You go in to report that your wing mirror has been broken and the car window has been smashed and someone has attempted to steal the car, most people will recognise that individual investigation is not going to happen. What the cops do is build up a pattern so that if every night or every Friday night for a certain period of time this is happening in a certain locality, then the police officers will do something about it. Often that will take out the person who is doing it. It goes back to what I was saying, you address the cause and not the symptoms. The same is true here. An example of what we have done recently within SOCA is that we were made aware of an attack that was going to be perpetrated on Internet banking sites. This is in the public domain now because we have referred to it and it will be in our annual report which has just been published. We made that information available through an alert to the banks and financial institutions; they were able to put the software devices in place to prevent it from occurring which meant that a lot of people carried on Internet banking without any threat or hindrance and never knew it had happened. What would have happened if it had gone through would have been a major problem with a great many people who would have wanted to report it. It would have seemed like small amounts but it would have amounted up to a huge amount of money. It was stopped from happening and that is what we are trying to do, get ahead of the curve rather than investigate it afterwards. There would be some difficulty chasing these guys after they have perpetrated the offence. The point I was making earlier on is that we do need to know about these matters so that we can build up a pattern and build up the intelligence and that is what the police unit that Sue is talking about is trying to do and what we are trying to do.

Q1068 ***Chairman:*** To what extent is SOCA already doing it for individual complaints? You talk about the wing mirror, is what you say actually happening with the equivalent in the e-world, if there is an e-Bay person who has lost £180?
Mr Hughes: the equivalent in the e-world is that that information is coming to us because of people like e-Bay who will collate that and bring it to us. Other people who collate it bring it to us. That is one of the reasons why some guidance has gone out recently about making sure that information is collated. When you report to your bank that you have been a

victim then it comes back in a collated pattern form we can do something about.

Q1069 ***Earl of Errol:*** How long has this been happening?
Ms Lemon: e-Bay have a wealth of intelligence around criminal activity.

Q1070 ***Earl of Errol:*** I know from friends who have been defrauded using auction sites that if they ring e-Bay then e-Bay say they cannot do anything about that particular fraud because if they did not pay through Paypal they are not interested. They suggest they report it to the local police; the local police are not interested in taking the report because the other person is under a foreign jurisdiction and so what you are describing does not happen. Even if they were to report it to SOCA it is not in your remit. Do you then parcel that back out to the local police force to do something because you are not responsible for level two crime across county boundaries within the UK if serious crime is not behind it?
Mr Hughes: You are misunderstanding what I am saying. The point is that what we are looking for and what we are creating with our colleagues and people in the private sector, is to build up that pattern and bring it back to us so that we can do something about it.

Q1071 ***Earl of Errol:*** If it is not serious crime you cannot, so what do you then do with it? Do you report it to someone else?
Mr Hughes: That is the point. What we are talking about here—as I was referring to with the fraud that went on—are very small amounts which build up into a large amount of money. Serious organised crime is not defined in the legislation that set up SOCA. The point is that what we are looking at is that which impacts seriously upon individuals, where it is clearly organised, where there is substantial financial profit or whether there is violence or other harm caused. Those are the issues we are looking at when these matters are reported to us.

Q1072 ***Earl of Errol:*** When I report that I have lost £500 to you at SOCA, if you decide it is not part of a serious organised attack and is something below the million pound threshold perpetrated by a few people in Britain, what do you do with that?
Mr Hughes: If those crimes are reported to us then we will refer you to your local police force. That is the issue we are talking about here.

Q1073 ***Earl of Errol:*** Will they do anything about it?
Commander Wilkinson: There would be an initial assessment of a report like that. You can quickly tell how difficult it is going to be and whether it is even going to be possible to identify the offender. Rhe Metropolitan Police on behalf of the other forces, works with e-Bay to gather intelligence pictures around particular trends and patterns. Once we have a good intelligence picture we can put a proper investigation, whether it is at a national or even at an international level working with SOCA then we will do so.
Ms Lemon: Just for clarity, if these crimes are reported to SOCA, where we work with e-Bay is because they have a very good intelligence base around the big criminals on e-Bay and that is where we engage with them.

Q1074 ***Earl of Errol:*** That is the reason I used it as an example because actually people do not and there is no mechanism to do it, therefore those crimes do not actually get reported.
Ms Lemon: To the local police they do.
Mr Hughes: It was a point I was making, that we need to find ways in which we can gather that information.

Q1075 ***Earl of Errol:*** It is not a SOCA task to do that, it is a police task, is it? This is an important distinction which is why the national centre is so important and it is not to do with SOCA, it is to do with the initiative led by Commander Wilkinson.
Commander Wilkinson: It may involve SOCA because it depends on the scale of the issue. e-Bay is an international organisation so we may need to work very closely with them.

Q1076 ***Earl of Errol:*** I realise you may need to but the new national centre and all the stuff we are talking about is not a SOCA responsibility.
Commander Wilkinson: Taking initial crime reports at a local level is the responsibility of local police forces. The purpose of the new ACPO police unit will be to coordinate what happens across the 43 police forces, not to take individual crime allegations but it will be to monitor crime patterns across the UK, across the ACPO police forces.

Q1077 ***Baroness Sharp of Guildford:*** Commander Wilkinson, you have spoken about the websites where people can report this.
Commander Wilkinson: Yes.

Q1078 ***Baroness Sharp of Guildford:*** Is there a website where you can report if you have been a victim?
Commander Wilkinson: The key one is the Fraud Alert website which is currently available through the Metropolitan Police website but is actually accessed by people nationally and internationally. We have something up to 15,000 reports a month. There is a disclaimer on the website to inform people that we will not necessarily send a reply to the e-mail nor will we necessarily investigate what we are being told

about, but what the public are doing is helping us to assess exactly what the intelligence picture looks like so we can tackle it at source much more effectively.

Q1079 ***Baroness Sharp of Guildford:*** Ideally what you want is for people to go onto that website and report it on the website rather than going round to their local police station.
Commander Wilkinson: Both. I would never want to discourage people from going to their local police station but the useful thing about the Fraud Alert website is that reports that appear on there are actually collated and assessed properly, subject to intelligence analysis and dealt with and prioritised accordingly.

Q1080 ***Baroness Sharp of Guildford:*** I live in Surrey and if I went to the Surrey Police website would I get directed towards this Metropolitan Police website?
Commander Wilkinson: I do not know but one of the things that I would like to achieve through the new unit is to ensure that all police forces are providing a decent quality of service to everybody across the 43 police forces. That is exactly the sort of thing that I would like to see standardised across the country.

Q1081 ***Baroness Sharp of Guildford:*** From your point of view that is precisely what you want. You want a single website where everything is logged and then you can actually tell if there is a particular trend emerging.
Commander Wilkinson: The ideal situation for me would be if there were a single web portal that anybody could go to in terms of fraud or e-crime and they could get in through that central website, if you like, and then be guided within there to Get Safe Online or to the Internet Watch Foundation or to the Fraud Alert website, whichever is most appropriate. They may seek prevention advice, they may want to report crime or whatever and be led to the right place through that single portal. That is certainly something that Sharon and I are going to work together on. I understand there are some technical challenges around it and it may cost quite a bit of money to do, but it is certainly the direction in which we need to travel.

Q1082 ***Baroness Sharp of Guildford:*** That sounds very sensible.
Commander Wilkinson: Yes.

Q1083 ***Lord O'Neill of Clackmannan***: We get the impression that this is a Metropolitan Police led thing; you do not know what happens in Surrey, for example. How consistent are skill levels across the police forces? Are there centres of excellence in the investigation of Internet crime outside of London?
Commander Wilkinson: We have done a very provisional capability assessment across the 43 police forces to provide part of the business case for the National Unit. We now need, through the National Unit, to go back and get a very good standard and capability assessment done so that we can begin to standardise the skill level across all police forces. Across the country there are some very skilled investigators, whether it be into forensics or whether it be covert Internet investigators or whatever and we have a good idea now of where they are to be found. We also deal with e-crime on a regionalised basis—given that police forces vary hugely in terms of size, for example, and resources available to them—and what we have done is publicised who is where, who has got what capability so that police forces around the country know where to go to get support and help. That is what we have been working on up to now.

Q1084 ***Lord O'Neill of Clackmannan:*** My colleagues were in the United States and they found that near San Francisco there was an FBI laboratory which was funded both centrally and from private sources. That provided very high level expertise in computer forensics. I am not sure that every police force within the US would be capable of benefiting from it, but those that could were able to do so. Would you envisage something of this nature happening in the UK where there would be a centrally co-ordinating network of skills and equipment to support regional police forces?
Commander Wilkinson: That would be an ideal scenario and would take some time to achieve I think. The important thing is that I get all police forces to a position where everybody knows where they can go to get the relevant expertise or support or help or advice that they need in whatever context to do with e-crime. That would be my first aim, to get to that position.
Mr Hughes: There are several issues at play here and the point you are making is that there is e-crime and there are also forces that have centres of excellence around the investigation and analysis of equipment seized during an investigation as well, people who are better placed to deal with access and the way that e-crime has been perpetrated. What we are trying to do is pull together all of that understanding of what is going on in police forces around the country so that we are able to deal with e-crime and trying to find a way of making sure we have the best analysis. Sometimes the unit that you are talking about at the FBI, the federal resources are there to support in different types of scenario. The ones that we have dealt with are those looking at crimes being perpetrated and then there will be other labs, as such, which are good at exploiting the evidence and intelligence that you gain from that equipment.

Q1085 ***Lord O'Neill of Clackmannan:*** What you are talking about does seem incredibly fragmented. This has been a form of crime that has been going on for quite a while. Is there not a case for making the resources of a national character, that you break down these 43 barriers?
Commander Wilkinson: That is entirely where I am coming from in terms of the business case that I put forward to the chief constables who all agree that a national unit is needed, or a unit covering the 43 police forces is needed to get standards, policy, training and skills levels standardised across the country. That is the whole premise for the new unit. I should just add—I do have one copy here that I can leave with the Committee—that ACPO does publish good practice guides and this one I have here is for computer based electronic evidence and evidence retrieval and actions that officers should take when attending the scene of an e-crime and how to handle computers, laptops, phones and that sort of thing. We do constantly keep these good practice guides up to date and circulate them across the country so there is also written support and policy guidance.

Q1086 ***Lord O'Neill of Clackmannan:*** With respect, this seems to be a rather top-up approach. Is there not a case for some kind of top-down approach? How do you get these 43 ferrets in the bag behaving themselves? It is akin to a bit of a shambles, is not really? You are doing your best but somebody needs to grab a hold of it and nobody seems to be doing that. I am not saying that you are not trying but ministers hiding behind business case excuses, that really is the most feeble excuse for a minister to utilise. They will always nitpick; they will always employ good accountants (or even bad ones, which is probably even better) to nitpick at the detail and you will get nowhere.
Commander Wilkinson: I would refute that to a certain extent because the 43 chief constables are now signed up to the National Unit and I think that is an enormous step forward. We are now entering the implementation phase of putting it together. I think everybody has recognised the fact that the 43 forces need to work together to be more effective in terms of the service that we provide to the public on e-crime. I cannot tell the 43 chief constables what to do, but what I do find when I speak to the 43 chief constables is that they actually see the logic and the sense in what I am saying and they acknowledge the service that the police service provides at the moment could be improved. That is what the National Unit is all about.

Q1087 ***Lord O'Neill of Clackmannan:*** Without the national centre or the network that you are working towards, how long do you think business will stand by and say, "We have this money ready"? Will they be on stand-by forever or will they say, "Look, if you don't come across with something sensible before long we'll just go away and do what we can as best we can" and you will lose the opportunity of private funding?
Commander Wilkinson: I may be living on a pink cloud here, but certainly the feedback I have had from industry is that they are extremely pleased with the speed with which we have got the principle of the unit agreed; they are ready with the money now and we have now entered the phase of actually going back to them and saying, "Show us the colour of your money; show us how you are prepared to support us". Over the next few weeks I intend to pull all that together into the business case that I have been talking about and take it back first of all into the Met because the Met is going to house the unit (the Metropolitan Police Authority) and then back out onto a national basis with ACPO and back to the Home Office.

Q1088 ***Lord O'Neill of Clackmannan:*** Good luck with that. Regardless of what might happen next week with the elections there are still six million people north of the River Tweed and unfortunately there are criminals there as well. There are nine police forces in Scotland. Do you talk to them?
Commander Wilkinson: Yes.

Q1089 ***Lord O'Neill of Clackmannan:*** I know ACPO is a UK organisation but there is a Scottish bit as well.
Commander Wilkinson: Yes, there is an ACPOS and actually Scotland are ahead of us. They do already have an amalgamated unit and there will be a protocol in place with them in exactly the same way as there will be one in place in SOCA to ensure that we are all working together effectively.
Ms Lemon: ACPOS are on the National e-Crime Strategy Group.

Q1090 ***Chairman:*** How many units are there? You say there is one in Scotland, is that of the same size and capability as the Met unit?
Commander Wilkinson: No, nothing like. I think it is more of a coordination unit but they do have a unit of sorts that coordinates the service that Scottish forces provide. The Welsh Assembly is also beginning to put a unit together to coordinate the Welsh forces. One of my key aims in putting the ACPO unit together is that I do not just duplicate what they are already doing. We must take advantage of where they have got to so I can concentrate resources perhaps more on areas that are not covered by units.

Q1091 ***Chairman:*** I would have thought there is a volume question and there is also a turn-around type question. If every bit of equipment you go in and grab you need to look at it fairly quickly and this is a time consuming business. When we looked at this in the

States I think the FBI has 12 units or something like that around the country. We are five times smaller but I would have thought you would need two or three units of the quality that the Met has but probably larger than the Met has. We were very impressed with what we saw at the Met but it was barely sufficient for London in my opinion, let alone having to take stuff from all over the country. I would have thought you would need three units in the UK.
Commander Wilkinson: Every force has access to a forensic lab and every force has access to digital retrieval facilities. I think the biggest problem at the moment is the backlog because more and more phones and computers et cetera are being seized as part of routine investigations. Another aim of the unit will be to get some proper criteria into place whereby cases are prioritised so that it is not seen as a massive backlog but we are actually bringing the more critical cases to the front of the list.

Q1092 ***Lord Harris of Haringey:*** Both in the US and here we have heard about the loss of support staff to private sector companies. Is staff retention a major issue for you and what are going to do to overcome it?
Mr Hughes: I think that is probably an area for us to talk about because the advantage that Sue has is that she has police officers as well doing some of this work but actually there are people that the Metropolitan Police and other forces have who are locked into a police service background. The answer to that is yes, we do have a problem about recruitment and retention. We are competing with the wages that are paid in the private sector. That will always be a problem. It is the same with financial investigators; it is the same with a lot of other areas where we are looking at changing the face of the work force for the police service and in the way in which SOCA operates. There are tactics and strategies that we are adopting in order to try to recruit and retain people. There are development strategies that we are using and ways that we bring people in and use them in projects. Many people in law enforcement do not do the job for the money because if they do then they have made a fundamental mistake. The point is that they do the job because they want to do it. Yes, we have a core of people who will stay with us but recruitment and retention is difficult. That is one reason why what we are doing is working with our private sector colleagues to see if they can supply us with people on secondment or by use of them assisting us with some of the expertise that they have. That is what we have to do in that type of environment.
Ms Lemon: We are looking at alternative methods as well. Previously if some evidence were seized it would be a digital evidence recovery officer who would have that kit and join a queue but now we have a triage system and we are looking at some good practice by some of our partners overseas who then make that available without any interference from the evidential trails to the operational officer remotely. They can then examine that disc for what they want and then we can back it up with the evidence trail. You do not need the expertise around that, just the initial expertise around the triage and then the operation officers get immediately what they need. That is some good practice from one of our partners.

Q1093 ***Lord Harris of Haringey:*** Is there a problem so far as experienced police officers are concerned?
Commander Wilkinson: There have been instances where that has happened. We also have a threat almost from people being promoted and therefore being posted into a different role which is rather infuriating. In my view it is a mixed economy and we can look more flexibly at how we pay our police staff to supplement the police officers that are in post and also my perspective is that we use industry. Most of our partners are very, very keen to help second people into us. If we are losing staff to them, at least we are getting very competent and experienced staff back on secondment. I think we just need to remain flexible. There is always going to be a situation where police wages and police staff wages are less than the going rate in the private sector; we just to be clever around it.

Q1094 ***Lord Harris of Haringey:*** Does that meant you are satisfied with the number of police officers and police staff you have available to work in this area?
Commander Wilkinson: I want to mainstream it remember, so I think the more I can do that the better value I can get out of every single member of the police force and the police staff who support that police force. We need to raise everybody's capability across the board. In terms of setting up specialist units I am not aware of any acute recruitment problems. People will come into it for a while at least. Of course it costs a lot of money to train them and we would like to retain them as much as we can, even on promotion.

Q1095 ***Lord Harris of Haringey:*** Are there serious backlogs of work in any of the specialist units that you are aware of?
Commander Wilkinson: There are backlogs of work in terms of forensic retrieval which I have already mentioned. The demand is endless on these units and it is a question of prioritisation, working out the crimes that are causing the most threat and harm and investing those. We are never going to be able to investigate it all.

Q1096 ***Lord Harris of Haringey:*** The Home Office at one stage provided central funding for two computer crime officers in each force. What has happened to those posts since the loss of the National High Tech Crime Unit?
Commander Wilkinson: I think you are referring to the Home Office funding that was divided between each force. It represented about £38,000 per force and it was withdrawn earlier this year as part of Home Office savings. That money is probably, if I dare say this, a drop in the ocean to most police forces. It clearly had more impact on the very small police forces who may have funded a post in computer crime investigation or whatever with that money. I certainly hope, through the National Unit, by other means to restore capability across every police force in the country.

Q1097 ***Lord Harris of Haringey:*** In principle the Home Office has £38,000 times 43 which it took out of its budget which it could put it back into the National Unit if it wanted to.
Commander Wilkinson: I would love it if that were to be the case; it would help me enormously.

Q1098 ***Earl of Errol:*** Recent guidance requires the police to refer victims of phishing fraud to the banks in the first instance, rather than the police logging them as crimes. What do you think of this?
Commander Wilkinson: I think it is a very helpful development because, as we have said several times during this session, individual reports to individual police forces about such phishing offences really do not give us a good picture of what is going on and it is impossible to get a proper crime pattern analysis as things stand at the moment. However, if all these reports are collated by the banks, who have very good support in terms of intelligence analysis, they are able to refer to us particular trends and patterns by collating right the way across the board and we get a much better overall picture. In general we are very supportive of this development.

Q1099 ***Earl of Errol:*** In the US the Federal Trade Commission has gone the other way. They are requiring offences to be reported in the first instance to law enforcement. That then triggers a crime number and everything, then it gets reported to the bank and the bank then triggers an investigation. Does that not make more sense because then you actually know what is going on?
Commander Wilkinson: We are getting a very good picture of what is going on through the banks. By reporting each individual one to a police force, given the scale of what we are talking about, it would increase the bureaucracy enormously.

Q1100 ***Earl of Errol:*** Would it not give more intelligence? You do not necessarily have to react to the things but it would give you the intelligence. Do the banks not have an interest in down-playing the level of these things?
Commander Wilkinson: I think the partnerships that we have with the banks, for example, are extremely good now and we are working with them—sometimes confidentially depending on the nature of what is going on—to get a good picture of what is going on. If everybody just reported their crime to the individual police force I do not think there is going to be much benefit gained because if you have thousands of victims of one particular crime right the way across the UK, given that there are 43 police forces, you are not going to be able to get an accurate, overall picture; the banks can.

Q1101 ***Earl of Errol:*** Surely this is where your national Fraud Alert site—if it were properly resourced and you had more than one person on it and you had the software developed for it—would answer this problem, should it be reported nationally to a single place. We have heard some evidence from Detective Superintendent Russell Day that financial institutions were not always reporting e-crime to the police either because it would damage their reputation or they knew you did not have the ability to cope. I do not know whether that is true.
Commander Wilkinson: The Fraud Alert website is feeding information into the banks in just the same way as various other sources are. That covers that. We do have police officers working within APAX and the Dedicated Cheque and Plastic Crime Unit and that is directly funded and run by APAX and by the Payment Clearing Services. Therefore I think the intelligence picture is transparently shared within the banking industry and law enforcement. The key thing here is that the scale of it is so massive we can only deal with a situation where a proper crime trend has been identified or a proper suspect can be located or whatever and through the collation, working this closely with the banks, we get a much better picture of what is going on.

Q1102 ***Earl of Errol:*** When we visited the States the FBI told us that a side-effect of data security breach notification laws was that more reports reached them since companies had to tell their customers in any case. Would you welcome such laws in the UK to give you better intelligence? A lot of data breach is going unreported in other words because people do not want people to know. Would it help your intelligence gathering if we were to have data security breach notification laws?
Commander Wilkinson: I cannot really comment because I have not had the time to think it through properly and clearly. It is quite a complex question. I

would imagine the scale of such breaches would be such that it would be very difficult to manage and I do think that the partnerships that we have in place with the banks and with other agencies such as the ISPs for example are good, they are robust and they are improving. I think that the intelligence picture is being shared in any case.

Q1103 ***Earl of Errol:*** In the States it covers companies as well such as TKMax for instance. The EU produced a directive on this in the summer.
Mr Hughes: It is a very interesting development. I am aware of these issues. It creates quite a lot of bureaucracy in the United States as the FBI will also tell you. Yes there are advantages. It is like all things, if you have a better picture of what is happening then you are better placed to be able to respond to it. We welcome all ways intelligence and information can be gathered. The danger of it is that if you stifle e-business by putting too many constraints upon them then what service are you also doing? You have to look at it from both sides. I know that is an unusual thing for someone in law enforcement to say, but if you make it so difficult or so restrictive then there will be an army of people who will find other ways round it as well. What we are looking at within SOCA is establishing good partnerships whereby in confidence we get the information that will help us to do something about it on behalf of the citizens and the bank customers and other customers without causing the banks or financial institutions to find themselves in such a bureaucratic tangle that they do not want to do it. It is a difficult balance to strike. I think it will be very useful to see your report on those issues and what the issue and how it works in the United States is. The issue that keeps coming back here is that the FBI is a federal responsibility and is funded in a separate way to how we are operating here in the United Kingdom. There are some differences there. There are obviously areas where we could pick up. What we are trying to do is coordinate what is happening in the United Kingdom already and try to make that a working model. I hope you wish us well on that.

Q1104 ***Chairman:*** We are looking at it from the point of view of the individual and the individual may not trust their bank. There are clearly examples where banks should not have been trusted and they did not reveal information they had for long periods of time. That was not in the interests of the individual.
Mr Hughes: No, I accept that.

Q1105 ***Chairman:*** That is what the American system is trying to solve so that the individual can turn to the people who should be enforcing the law, be their help and their friend there, and they are not necessarily going to have to deal with somebody whom they may suspect themselves. I am not saying for one minute that the banks are necessarily doing anything that is against the law, but we have had cases in this country where the banks have not disclosed, for considerable periods of time, information that was in the interests of the consumers to know. That is why I think, certainly talking from my own personal point of view, I doubt this position that the individual is told it has to go to the bank first; they should go to you first.
Mr Hughes: That is why we work very closely with the regulators, the FSA and others to make sure that we are getting the accurate and full picture. It is back again to resourcing and how best we can address the issues that are raised. We need to find ways of doing that and we are not saying we would expect individuals necessarily to put their trust in other institutions. We are not saying that. It is where we can establish good working relationships in regulated industries, where we can get the information that we need in order to combat those who are impacting and causing harm to the communities in the United Kingdom. We have to look at every way we can to find that.

Q1106 ***Earl of Errol:*** Does it concern you, Commander Wilkinson, that you could end up with a national crime unit which is funded by the private sector entirely if the Home Office and government do not come in and jointly fund it?
Commander Wilkinson: That is a theoretical possibility yes. I do not know what it is going to look like yet because this is exactly the phase we have just moved into, the actual funding of the unit and where the money is going to come from.

Q1107 ***Earl of Errol:*** We could end up with a privately funded part of the police service.
Commander Wilkinson: It may start off as being largely privately funded. The Metropolitan Police, by virtue of the role it plays in terms of investigating level two crimes, already puts considerable resources into it. They are largely unseen but represent at least half a million a year, probably about a million. We are taking that into account with the business plan. What I would like to see is that if it goes into the National Community Safety Plan that eventually it is taken out of the top slicing from all the police forces. I think the way e-crime is going, the nature of it and how it is becoming all pervasive in lots of different types of crime, there will come a point where all police forces could contribute into the national unit because it is affecting them all so much.
Mr Hughes: There are very clear guidelines on all forms of sponsorship and when police forces or law enforcement agencies are inspected they will look particularly at those guidelines to make sure they are properly in place and properly managed.

Commander Wilkinson: There are several parts of the Metropolitan Police for example already that are either wholly or partly sponsored by private industry. It is not new territory.

Q1108 ***Chairman:*** What is your experience of the quality of international cooperation in investigating and prosecuting e-crime?
Ms Lemon: My experience is that this is a necessity; it is not an option to have good relations with our international partners in this crime type. From the very first days of the NHTCU which has carried on to SOCA e-crime we have established some exceptional working relationships with our international partners. I can give examples of where we have used leverage of our relationships with other countries. For example, my counterpart in Australia needed to get into a country nearer us and I have a good relationship with that country and was able to afford the introduction on an operational basis which had a successful conclusion. More recently exactly the opposite happened where he had a very good contact on the other side of the world in Asia, I needed to make use of that for an operational reason and that saved opening new doors, creating new relationships and we were able to work together very effectively. We held the e-crime congress in the UK in this year. We invited 25 countries; 20 countries attended. We had a bespoke law enforcement e-crime day which was the first of its kind which was very, very encouraging and gave a lot of countries which would not normally have had an opportunity to speak on an international platform that opportunity. While it was very humbling because they were so grateful, it was extremely informative because some of the countries which might be overlooked have great skills and experience from which we can learn. We have the G8 24/7 network; we have the botnet taskforce; we have taskforces around the world for specific e-crime offences; Digital Phishnet; the botnet. Also we have a series of attachments within SOCA and we are trying to create new jobs and techniques and there are other countries who are way ahead of us so we have them attached to our unit on semi-permanent basis so we are starting from a greater distance in than we would have previously. So far as I am concerned, the legislation we mentioned earlier can be problematic but despite that I think it is extremely encouraging.
Mr Hughes: We have good examples of work for example with the Russian and the Chinese and that has been very helpful. We have an international liaison network within SOCA which is now the second largest in the world after the DA in the United States of crime liaison officers. They are there for the whole of the United Kingdom and not just for SOCA. We have embedded 23 of them within other agencies in other parts of the world with whom we have strategic alliances such as the RCMP in Canada, the BK in Germany, et cetera. There are a lot of areas where dynamically we can move a lot quicker than we ever could in the past in order to take forward law enforcement. That service is available to all police forces in the United Kingdom (it includes Scotland and Northern Ireland as well).

Q1109 ***Chairman:*** Collaboration is reasonable within the EU, is it? Would there be any point in establishing EU cyber police?
Mr Hughes: We hold the Europol Bureau on behalf of the United Kingdom and the Interpol Bureau. Working with Europol we have a significant number of officers where all of these matters are brought together. They have analytical working files on behalf of all the EU countries around particular types of crime and cyber crime. E-crime is one of those areas that Europol work on. So we already have that sort of linkage across Europe. In parts of the world that have already been referred to such as the United States, Canada, Australia, these are not major problems. In some parts of the world it is more difficult but we are still working with those parts of the world to establish good relationships and good investigation practices.

Q1110 ***Chairman:*** Which are the countries that give us real trouble?
Mr Hughes: I think you mean the individuals within certain countries who cause us trouble.

Q1111 ***Chairman:*** Not necessarily. Some countries presumably are quite uncooperative in terms of following up on leads that we might provide to them about resources and bad practice.
Mr Hughes: We have not found too many countries who are reluctant. Often they have problems about resourcing and about expertise. As I said just now, we have worked and are continuing to work with the Chinese Ministry for Public Security. In fact Sue and myself were in China recently making sure that the relationship with the Chinese authorities was of a very high order and has improved remarkably and we were getting very good relationship building there. Again the same with the Russians where we work very closely with their Federal Drugs and Crime Units and with the MBD in Russia so we are not seeing major problems there. There are certain parts within Eastern Europe which are difficult to access for various reasons, but that is not preventing us too much at the moment. I would be reluctant to name individual countries because in some instances they have not had the full opportunity to cooperate with us.

Q1112 ***Chairman:*** How do you resource this?
Mr Hughes: This is very expensive.

Q1113 ***Chairman:*** It must be very manpower intensive.
Mr Hughes: Yes.

Q1114 ***Chairman:*** You cannot send in teams of people to work with the Chinese presumably; you do not have the people to send, do you?
Mr Hughes: We have officers working there but what we do—this is the point of what we are trying to do about embedding—is to work with other agencies in a global alliance as it were so that other countries see the benefit in working to help us with a particular issue that impacts on the UK on the basis that a quid pro quo applies and we will help them when they have an issue, such as the point that Sharon was referring to just now with her colleague in Australia. It is about forming good working partnerships and alliances and that is an area where particularly the SEO have helped us enormously. The ambassadors overseas their second highest public service priority is around supporting the work against combating serious organised crime. The support we have had from ambassadors around the world has been of a very high order. Again the consulate services in China put themselves at our service and were very, very helpful to us. You are right, it is resource intensive, but we will only get results if we work in that way.

Q1115 ***Lord Howie of Troon:*** Are there some countries where the proportion of ill intentioned villains is higher than others? You probably know this.
Mr Hughes: Yes.

Q1116 ***Lord Howie of Troon:*** Are you going to tell me?
Mr Hughes: It does not always help to publicly identify those countries but yes, there are problem areas and you will find they are areas, perhaps countries, where there is very low employment and a very high number of people with certain skills who are now putting those skills to other uses. That has been the case within certain parts of Eastern Europe.

Q1117 ***Lord Howie of Troon:*** Do you have a black book or a book of any colour somewhere with this in it?
Mr Hughes: I never carry it around. It is one of the points that we need to make with our liaison officer network. We have liaison officers in parts of the world that are very difficult and they do a very difficult and demanding job. It is one of the areas that we are trying to break down.

Q1118 ***Lord Howie of Troon:*** You do know where you are looking.
Mr Hughes: Yes.
Commander Wilkinson: The only thing I would add is that some countries just do not have the legislative framework within which we can fully operate. They are willing to help but it may be the offence we are talking about is not an offence in their country or they do not have the powers that we have to intervene. I think that is worth outlining.

Q1119 ***Earl of Errol:*** There are a lot of websites out there providing advice on on-line security and safety, opportunities for victims to report crimes and so on. What is being done to map such sites and to ensure that in future there are fewer, more authoritative, higher profile sources of information?
Commander Wilkinson: I am very proud to be a member of Sharon's National e-Crime Strategic Group that she chairs as SOCA and I sit on as the ACPO lead on e-crime. The Met has taken a tasking from the group to map those websites—we know there are 200-plus—to actually look at them to quality assure them and to come up with a strategy about how we can map the sites and come up with a proper portal system, making it more coherent for the public generally. We are in the throes of doing that.
Ms Lemon: I think we have a lot to learn from the work that is being done by Jim Gamble and the Virtual Global Taskforce where most sites now relating to child abuse or child issues on the Internet can be easily found and are linked to each other. There are a lot of parallels there and we just need to coordinate them.

Q1120 ***Earl of Errol:*** I think it would be useful if people could know where to go.
Ms Lemon: Absolutely.
Commander Wilkinson: If you look on the Fraud Alert website already that kind of guidance is available through that website as it is through several others. The point is to bring them all together and communicate it well so that the public generally understand where to go. I think the problem at the moment is that they do not necessarily understand where to go.
Mr Hughes: The analogy with the CEOPS centre is sensible because if you are a child and you are on these Internet chat sites and various groups and domains that are set up then they will have the Virtual Global Taskforce sign and it is this push/pull: do people have to go looking for it or is it brought to their attention? What we are looking at are ways in which we can perhaps link those. For example, to pick up a point you were making just now about the way that the American legislation has gone, if you are on you banking site doing your

Internet banking then perhaps there ought to be a sign there for where you go rather than you having to go looking for something in order to make a report. Obviously with police force websites and SOCA's websites we can perhaps indicate where people can go, but they have to go looking for it, whereas if they are doing their Internet banking and if it is on their e-mail ISP provider's site "Here's where I go to report a crime" then that maybe the way we need to go in the future.

Commander Wilkinson: To be fair to the ISPs, a lot of this information is on their websites already and as soon as you call it up on your home page the advice is there and the warnings are there. We work closely in partnership with industry to further that.

Q1121 ***Chairman:*** We have come to the end of our questions. Thank you very much indeed for your input. It has been very valuable and very useful to us. Should you think of anything that you think we should know as we come now to writing our report and the recommendations, then please let us know.

Mr Hughes: To reciprocate on that, if your clerk wants any assistance from us then we are more than happy to provide that in any way we can.

Chairman: Thank you all very much.

Written Evidence

Memorandum by AOL

About AOL in the UK

AOL is a leading provider of digital communications and content to UK consumers. AOL offers dial-up, broadband, voice and portal services and has more than 2.2 million subscribers in the UK, including more than 1.4 million on broadband.

AOL subscribers in the UK spend more than two hours a day on average connected to the Internet. The AOL service and portal deliver a range of market-leading online content, including music, film, sport, news, shopping and community, as well as email, instant messenger, VOIP, safety and security features. AOL is also one of the leading online destinations for advertisers in the UK.

The AOL branded services are supplied to UK subscribers by AOL Europe Services SARL, a company in the AOL group based in Luxembourg. AOL (UK) Limited provides marketing and other support services. Both companies are part of AOL Europe, a business unit of AOL LLC, which operates a leading network of Web brands and is a majority-owned subsidiary of Time Warner Inc.

AOL's Outlook on Personal Internet Security

With almost 70% of UK homes having an Internet connection and time online rising, it is clear that UK citizens are embracing all the great things the Web has to offer.

While the Internet is enhancing the way people communicate, work, buy and sell goods, find information and access public services, AOL accepts that the scale and pace of change is true for both the good and bad aspects of the online world.

The wellbeing of Internet users has always been a priority for AOL and, as Internet penetration increases and more people shop, bank, meet other people and carry out other activities online, AOL recognises that PC protection is now more vital than ever.

AOL's commitment to Internet security includes providing tools and services, publishing detailed advice for users, and working with industry, Government, law enforcement and other stakeholders.

A Summary of the Risks

As technology becomes more sophisticated, so too do the criminals. AOL strives to keep its subscribers updated about the potential risks and to provide tools to help reduce them.

The Web has changed the face of commerce and most retailers now have an online presence. AOL's Brand New World study shows that 60% of UK adults buy some goods, services or tickets online. There are clear benefits to online shopping, such as the convenience and the ability to compare prices, but it has also brought new dangers, such as the fraudulent use of credit cards.

Using the Internet we can now find information on anything we want. But it also means anyone can find out about us. So, Internet users need to be aware of the potential privacy risks when putting their personal information into websites and other online forums.

Unsolicited junk email, or spam, is one of the primary concerns. Spammers are increasingly using more sinister tactics, such as employing zombie PCs and bot-nets, to hide the source of the spam and tricking consumers with special order spam, which claims to be from a friend or part of a legitimate, customer-driven transaction.

Such online scams and hoaxes appear to be on the increase. Phishing, for example, is designed to fool users into revealing personal information like passwords, credit card details and account numbers for criminal gain. Phishers send out millions of emails and set up cloned Web sites that look as if they are from trusted companies, such as banks and retailers.

Spyware refers to pieces of software that install themselves on the user's computer without their knowledge, usually when they click on a Web link or download a file. If users don't have protection against it, their Internet connection can be stolen, their preferences changed and their computer slowed down. More seriously, spyware can steal users' personal information, putting them in danger of identity theft.

Hackers, spybots and other Internet invaders are constantly scanning the Internet for PCs to infect and disrupt. Without firewall software, a computer is vulnerable every time the user goes online, particularly if it has a broadband "always-on" connection. A firewall places a barrier between the Internet and the user's PC, helping to prevent unauthorised access.

Computer viruses are software programmes deliberately designed to interfere with computers, disrupt or delete data and spread themselves—via email, downloads and files—to other computers. Viruses can arrive via a corrupted disk or program, email attachments, installing software, and in every kind of Internet download. Any information stored on the computer, such as documents, files or music collections can be lost in a virus attack.

It is clear from the above summary that Internet users face a myriad of potential security threats. For many consumers, this can make the Internet and computers seem daunting, especially if they have little experience of technology. AOL believes it is crucial that these issues are discussed openly and backed up with pertinent advice and robust technical solutions.

Consumer Understanding

Unfortunately, it appears that Internet penetration and advances in technology are outpacing consumers' understanding of potential online dangers.

In March 2006, AOL commissioned Populus Research to investigate UK consumers' awareness of, and the action they have taken to avoid, Internet security issues.

The study of over 1,000 UK adults found that although their awareness was higher than ever, most still do not do enough to protect themselves when they are online.

Understanding of Internet security terms such as phishing, trojan, virus and spyware had increased over the previous 12 months, with most respondents claiming to know what they meant. However, even though 86% said they are concerned about Internet security, less than half use specialist software to protect their computers.

AOL is committed to engaging UK Internet users on the issue of Internet security. As part of this, AOL has been running a campaign called/discuss since January 2006, the aim of which is to ignite debate on a series of topics related to the Internet.

The /discuss website has had more than 250,000 unique visitors since its launch, a number of which have commented on security issues. We have selected two examples for the purpose of this submission:

> *"I would guess now that 75% of all viruses are from people doing something incorrect, or stupid . . . such as downloading .exe files from a P2P sharing network . . . or opening junk mail, or visiting porn websites (which often contain dialers and more) . . . If you use the Internet correctly then your details are safe . . . Forget the firewalls, anti viruses, anti spam, etc . . . all you need is some common sense, and a little experience or training."* From the discussion forum "Is the Internet the ultimate invasion of privacy?" 22 June 2006.
>
> *"If I shop from the net, I will ONLY shop from sites I know are widely used and that have had great reviews . . . and not once have I been swindled for my money, but once, the ONE time I did buy from a site I'd never heard of before, the money got sent out, but my item never did . . . Just be careful who you buy from."* From the discussion forum "Internet shopping. Browse, buy or get mugged from the comfort of your own home." 12 February 2006.

Tackling the Issues

AOL believes that Internet safety and security is the shared responsibility of industry, Government, law enforcement and users.

As a leading provider of digital content and communications in the UK, AOL is committed to helping to protect Internet users by providing tools and services, advice and support, and working closely with other stakeholders.

Tools and Services

Spam protection

In 2005, AOL blocked an average 1.5 billion spam messages each day before they reached subscribers' in-boxes. AOL subscribers were engaged in helping us helping them so we could build an efficient tool to report and block mails which are considered by our users as spam. A user can report unsolicited emails to AOL without opening them, using a Report Spam button. AOL bases its filtering on the more than one million reports it receives each day. In addition, AOL subscribers can block messages containing certain words and filter suspected spam to a separate folder for sorting at their leisure.

Spim protection

For protection from the instant messaging form of spam, AOL's innovative IM Catcher automatically captures Instant Messages to highlight to the user that the IM is from unknown sources so that the user can choose whether to view them, ignore them or block the sender.

Phishing protection

AOL proactively blocks many known phishing websites and continues to launch legal action against spammers and phishers to try to hit them where it hurts—financially. AOL has pursued spammers in the US relentlessly and has found new ways and technologies to combating such activities and has also shared with our users some of the assets seized thereby driving better engagement.

Spyware protection

AOL's free Spyware Protection service scans the user's PC and offers four levels of protection, including checking for more than 28,000 known types of spyware and adware, empowering them to find and disable a wide range of threats.

Firewall software

AOL Broadband users get McAfee Personal Firewall Plus free as part of their monthly subscription to help avoid the threat from hackers.

Anti-virus software

As many viruses arrive via email, AOL provides free email virus scanning through McAfee VirusScan. All incoming and outgoing emails and attachments are scanned for viruses, worms, trojans and other infections and the software can be scheduled to automatically update on a weekly basis. AOL also recommends that users get a full anti-virus service to protect their whole computer.

Identity theft

AOL gives subscribers seven email addresses and recommends that a different one is used for personal emails to the one used in public areas of the Internet like chat rooms and message boards. This can help to reduce the risk of strangers contacting them or accessing their personal information. In addition, AOL provides advice about setting up complex passwords that are easy for the user to remember but not for others to guess and also encourages subscribers to set up an Account Security Question.

Computer check-up

AOL Computer Check-up assesses the overall health of the user's computer. It checks things like the browser settings and free hard drive space, diagnosing and automatically fixing any common ailments before they affect the PC's performance.

Advice and Support

AOL publishes extensive information about Internet security within the AOL subscription servic.

In 2005, AOL launched the Safety and Security Centre in the UK, which brings together all the safety and security features in one place, alerting users to potential risks and giving them more control over their time online. As well as links to the relevant security products, the area includes a Question and Answer section and an A-Z of safety and security terms.

We pay particular attention to children by encouraging parents, when they set up a screen name for their children, to use our award winning parental controls software to make sure that children have a safer and more enjoyable online experience.

In addition, AOL provides links to security information from relevant online news stories. For example, if there is an item about a new virus on the AOL News channel, subscribers can click on links within the story to access advice about how to avoid viruses.

Stakeholder Co-operation

AOL is a member of the Internet Crime Forum, a group composed of Internet Service Providers, law enforcement and data protection officers and the Internet Services Providers' Association (ISPA), for example. This group works with different stakeholders in Internet security and Internet crime yo help protect online consumers.

Through the Home Office Task Force on Child Safety on the Internet, ISPs, law enforcement, NGOs and other stakeholders look at ways in which the Internet and ISP tools are being used to put children at risk and have developed guidelines and frameworks for ISPs and content providers to help better protect children.

AOL is also very active in international pan-industry working groups seeking to develop better technology and standards both for the industry and its users.

Through ISPA, the industry has been helping to push the debate and actively seeking to engage all stakeholders and supporting UK Government policy around this issue.

Governance and Regulation

UK Government has been very active through the DTI, Home Office and Law Enforcement specialist units in supporting ISPs through policy and advice initiative to reduce security threats. Initiatives such as the DTI Working Group on Spam, the Home Office Task Force on Protection Children on the Internet, the Internet Crime Forum and the Get Safe Online projects have helped the dialogue between all relevant stakeholders.

We have seen that by all parties working together can help reducing the risks faced by consumers whilst allowing new technologies and standards as well as education material to be developed in a timely manner. AOL supports the UK self-regulatory regime and multi-stakeholders' approach.

Crime Prevention

AOL supports the current legislative framework which has helped clarify access and request to information from ISPs (Regulation of Investigatory Powers Act), allowed for some better understanding of grounds upon which ISPs can fight malicious and harmful security breach onto its service (Computer Misuse Act) but we would welcome more stringent remedies against spammers.

AOL has participated to two G8 meetings on eCrime and has found it most useful in bringing understanding and sharing best practice from other territories' industry, law enforcement and policy makers and would welcome similar events to be organised by government.

Conclusion and Recommendations

In summary, AOL believes that the good of the Internet outweighs the bad but recognises that consumers face a broad range of dangers. The company's focus is therefore on education and empowerment—educate consumers about the potential risks and empower them to minimise the likelihood of them occurring.

AOL's recommendations are therefore:

- ISPs have a responsibility to their customers: It is no good just telling users that protecting their computer is as vital as locking their front door, the onus is on the Internet industry to help provide the keys. And the keys must be regularly updated to keep up with new threats.
- Collaboration is crucial: AOL is keen for the Internet industry to continue working with government, law enforcement and other stakeholders to help educate and protect Internet users. Membership of joint taskforces and other bodies should be maximised.
- Self-regulation works: It would be useful to look at the model used to reduce the number of child abuse images available on the Internet. ISPs and other organisations have worked closely with the Internet Watch Foundation to help tackle illegal Web content.
- Striking the right balance is key: New Internet users in particular may be put off by scaremongering about security risks. It is vital that any awareness campaigns focus on the positive elements of the Internet too and that confusing technical jargon is kept to a minimum.
- Peer education is powerful: AOL's /discuss campaign is proof that online communities can be used to provide information and peer advice on issues such as Internet security.

23 October 2006

Memorandum by Apache

What is the nature of the security threat to private individuals? What new threats and trends are emerging and how are they identified?

Phishing, malware and disclosure of personal information.

Modern malware includes keystroke loggers (generally used for phishing), spybots (generally used for unwanted advertising, but also for phishing) and botnets.

Botnets are of particular interest because they are not generally targeted at the owner/user of the computer, but rather at third parties, with the user as an unwitting accomplice. Botnets have various uses, the most common being to send spam and to execute distributed denial of service attacks.

Because the user is not the target, it is entirely possible for the user to remain unaware of the presence of bots on his machine. Often bots are identified instead by the user's ISP or by victims of the bot.

Disclosure of personal information seems to be on the rise—a great example was AOL's recent publication of search history, supposedly anonymised, many of which were then linked back to the people performing the searches simply be looking at what was searched for. Another example that occurs regularly is compromise of users' credit card details.

The interesting thing about this threat is that the user has almost no way to mitigate it, other than not using the Internet for search or commerce—which rather defeats the point of the 'net.

What is the scale of the problem? How are security breaches affecting the individual user detected and recorded?

The scale is enormous—for example, estimates of botnet size indicate that there are nets of up to a million machines under the control of a single person, and that a significant percentage of machines on the Internet are infected (I have heard estimates as high as 25%).

Security breaches affecting individual users are often not detected, and almost certainly not recorded. Certainly there is no consistent framework for such recording.

What can and should be done to provide greater computer security to private individuals? What, if any, are the potential concerns and trade-offs?

Pursuing the perpetrators of attacks on users with more vigour should lead to improved security.

Often suggested, but in my opinion wrong-headed, alternative is to make software manufacturers liable for security breaches by their users. This seems to me to be the wrong approach for at least two reasons:

(a) It favours large companies over small ones.

(b) It is entirely incompatible with the increasingly important open source model for software: since this is largely created and maintained by volunteers for no direct gain, liability for security issues would probably vastly reduce the availability of open source software.

However, encouraging users to use more secure software, perhaps by publishing security metrics would seem to be a good idea, though I do fear that this would be manipulated by those with large budgets to make their software appear better than it actually is.

What factors may prevent private individuals from following appropriate security practices?

The main factor has been shown to be that individuals just don't care about security. That is, if you ask them to spend money in order to be more secure, generally they will not. This is particularly true for privacy, where studies have shown that users will sacrifice privacy for rewards as small as a chocolate bar, and are generally unwilling to pay anything at all for improved privacy, at least until something bad happens to them (when, of course, it is too late).

What role do software and hardware design play in reducing the risk posed by security breaches? How much attention is paid to security in the design of new computer-based products?

The hardware design required for security is largely understood (except, perhaps for the digital rights management kind of security, which works against, rather than for, the user) and consists of facilities in hardware for compartmentalising individual pieces of software from each other. Once this is achieved, security then becomes purely a matter of software. Most modern computers have everything required for software to be secure.

However, all prevalent operating systems and most of the software run on them, are not designed with security as a primary goal—indeed, they all derive from systems where users were largely trusted, as was the environment the machine runs in. It is exceedingly hard to "add security" to these existing, inherently insecure, frameworks—which is why we seem to have made no progress at all in the last decades on improving security.

In my experience (and my job is to do security reviews of new products) the attention paid to security is highly variable—designing for security is a specialised skill, not easily acquired, and many do not have an aptitude for it. Also, many companies see security as a barrier to fast release times and flexibility and ease-of-use and so deliberately do not prioritise it.

How effective are initiatives on IT governance in reducing security threats?

The main problem with IT governance as a means to reduce security threats is that governance is national and security threats are not.

A secondary problem is that the easy target for governance is the manfacturer or vendor of computer-based products—but this works against small organisations and open source, as I've mentioned above.

How far do improvements in governance and regulation depend on international co-operation?

It seems to me this is absolutely vital. As we've seen many times, making something illegal in one country just drives the perpetrators to other jurisdictions and does nothing to help the users.

Is the regulatory framework for Internet services adequate?

It seems to me that regulating Internet services has nothing to do with improving security. One of the problems with malicious versus legitimate activity is that they look the same. Only the outcome distinguishes them.

What, if any, are the barriers to developing information security systems and standards and how can they be overcome?

The biggest barrier is a huge quantity of legacy software which cannot have security retro-fitted. Improving security radically really requires starting again from scratch, redesigning operating systems from the ground up, and rewriting all of the software that runs on them.

This is obviously a massive undertaking—and becoming more massive every day.

Memorandum by the British Computer Society

Introduction

The British Computer Society (BCS) is the leading professional body for the IT industry. With over 56,000 members, the BCS is the leading Professional and Learned Society in the field of computers and information systems.

The BCS is responsible for setting standards for the IT profession. It is also leading the change in the public perception and appreciation of the economic and social importance of professionally managed IT projects and programmes. In this capacity, the Society advises, informs and persuades industry and government on successful IT implementation.

BCS is determined to advance IT knowledge and deliver professionalism at the highest standards by "Creating the IT Profession" for the 21st century.

Defining the Problem

1. *What is the nature of the security threat to private individuals? What new threats and trends are emerging and how are they identified?*

There are four main threats to the individual:

- Loss of the use of information on their computer.
- Disclosure of information to third parties which the citizen does not want—most obviously by persons gaining access to the citizen's computer by any means including physical theft or loss of the computer.
- Use of personal information to the detriment of the citizen (which may follow on from disclosure).
- Use of the citizen's machine for purposes the citizen does not wish.

This may manifest itself as:

- Internet: Malicious code including viruses, worms, trojan code and spyware. Also remote "bot" code, whereby the citizen or organisation becomes an unwitting conduit to (often illegal) acts such as becoming the source of distributed denial of service attacks, or the provision of storage/ distribution of material.
- Email: Spam, phishing attacks (designed to cause the unwary to part with confidential personal information, and spurious offers (designed to part the unwary from their assets by offering large fees to permit money payments through their account, highpaying jobs requiring no effort, etc). In many cases spam can account for more than 50% of a user's mail.
- Phones and mobile phones: hacking, eavesdropping, rogue calls from numbers operating a high cost return call, incentives to call highrate premium numbers.
- Wireless access: Often not secured out of the box, and generally not understood by private individuals.

New threats emerge with new technology—for example, as phone and PDA technology mertge, the interest in attacking "intelligent" phones will increase. VOIP (Voice Over Internet Protocol) will come under increasing attack as its use becomes more widespread.

2. *What is the scale of the problem? How are security breaches affecting the individual user detected and recorded?*

It is difficult to know the scale of the problem, as many user issues are not reported, and indeed it is often difficult to know to whom one should report ones concerns. However, it is accepted within the industry that the UK is a major (if not the major) source of remote "bot" Distributed Denial Of Service attacks, and this is an unintended consequence of large scale broadband uptake with relatively little awareness on the consumer's part of the risks involved.

The threats as such probably remain fairly constant, but with the increasing globalisation of the Internet and the increasing number of subscribers worldwide, the number of people who are potential victims and the number of potential attackers who could gain (legitimate or illegitimate) access to IT equipment and to the information they contain increases.

The citizen or organisation may run programs (eg antivirus, antispam or antispyware programs) to check for unwanted content in the stored data and programs on their computer (such programs may not be up to date at any point in time). However, if unwanted content is detected the citizen probably does not record that but merely gets rid of the offending item. Were every citizen to report these events to the authorities it is doubtful if the authorities could cope with the avalanche of reports.

What is not (readily) available to the citizen is the ability to detect if his/her computer has been taken over by the illintentioned.

The technical means by which illintentioned people may access the citizen's computer will vary with the software in use. The software will continue to contain bugs, legitimate functionality will continue to be misused and there will always remain the unknown vulnerability in all software; therefore at any point in time the citizen's computer remains at risk even if the citizen had done everything that the IT experts said they should do.

3. *How well do users understand the nature of the threat?*

An assumption could be made that novice users are unaware, and more experienced users become aware via news reports, service provider notification, and exchange of information between communicating users. Many users may have knowledge of security threats, but at the same time may have little appreciation of the implications to themselves, or any appreciation as to what they might do to mitigate such risks.

Websites run by both Government and the private sector try to educate the user, but these are "pull technology" and require the user to go looking for the information they contain. Often the user will not recognise the need to look in these areas, despite considerable marketing effort.

There is some anecdotal evidence that there are both timid people who won't use any part of the system because of the publicity given to the risks, and paranoid users whose reaction to security threats is extreme and disproportionate. Both extremes are a problem, in different ways, and neither understand the meaning of the information on offer.

Often, awareness is coloured by folklore. For example, there is no known case of a credit card being intercepted whilst being sent on the Internet. It is just too difficult to achieve. Conversely, there are many cases where vendors with poor security have exposed their customer's credit card records, with disastrous results. Yet the belief persists that the transmission is the risk, rather than supplier security.

Tackling the Problem

4. *What can and should be done to provide greater computer security to private individuals? What, if any, are the potential concerns and tradeoffs?*

Private individuals are not likely to have the same levels of security and technical support that users in organisations have—if there were some way of providing this to users it would help (but for user uptake it would have to be at low cost both in the financial sense, and cost of time to the user). Existing takeup on such services as are already on offer through ISPs is unknown but suspected to be low.

Technical remedies can be helpful, but usually impose both a financial burden and technical difficulties (regarding compatibility and configuration on systems that are individually customised). Security measures such as passwords have limited use as a security measure, as most users (private individuals and the workforce) do not follow password advice (on combinations, and making regular changes to passwords) if it becomes arduous.

5. *What is the level of public awareness of the threat to computer security and how effective are current initiatives in changing attitudes and raising that awareness?*

In absolute terms, the answer to this is unknown. It is generally accepted that the level of awareness amongst the user community is low. So also is the level of interest in the subject. There is at least a strand of thought which would suggest that it will always be low, and that education of the user is a last resort and an admission that technology has, as yet, no answer.

However, the security issues can be mitigated if not solved by technical means, given a willingness to do it. In the long term, products must be secure and capable of protecting the user against themselves.

6. *What factors may prevent private individuals from following appropriate security practices?*

In general terms, the following apply:

- Cost—all the security programs are extras often with annual charges. There is a cost in time to install and maintain them.
- Complexity—people may not understand how to use security features and/or misconfigure them.
- Forgetfulness—people simply forget to back up or run the security software.
- Cognitive limitations typically users will resort to easily remembered security processes. For example, despite guidance they will choose weak passwords, keep written records of passwords, and use the same password as far as possible for all communications/transactions. Most encryption products, where used, are highly secure, yet the user's private keys (which ultimately drive them) are protected by simple pin or password combinations which are extremely weak.

Often a lack of awareness that the dangers apply to them, and/or lack of knowledge in security management may mean that users may opt for risk, rather than cumbersome and inconvenient security practices.

7. *What role do software and hardware design play in reducing the risk posed by security breaches? How much attention is paid to security in the design of new computerbased products?*

Manufacturers of operating systems or hardware suppliers should play a major role but the results of their efforts may not be efficiently utilised by users, or by the technical configuration of the user machine. At present, dialogue boxes requesting input from the user often do not provide the information the user needs in order to make a sensible decision, but invite a "yes" answer to vaguely worded questions, even in the face of potential threats, thus negating the power of the product.

Manufacturers could supply all machines with appropriate prevention and detection software as standard. These, together with other standard software packages, would need regular updating which, using the Internet, is not a problem (providing updates do not disrupt settings in the computer). Manufacturers must make the security products easy to use, and provide mechanisms to detect misuse.

This suggestion raises commercial issues for the suppliers of software and possibly competition issues if the number of suppliers is limited on a worldwide basis. For example, whilst the security community in general welcomed the security measures inbuilt into the new Vista operating system, the decision of the EU to force Microsoft to "unbundle" security measures in Vista in favour of the commercial interest of competing vendors could be seen as counterproductive.

User psychology pitched against security infiltrators is a major security issue.

8. *Who should be responsible for ensuring effective protection from current and emerging threats?*

Ultimately, only the user can do this. Manufacturers, service providers, computer stores and internet sites can advise, cajole and even try to insist upon secure behaviour, but they cannot enforce it.

Communications gatekeepers (ISP's, telecommunications providers) are in the best position as the link between the user device and the "outside" world—however, to "ensure" effective protection they would need to be "assured" that user devices have the technical capabilities required and that users have an understanding of good security practice. This may not be feasible.

Protection will always cost, and users will always reserve the right to reject the advice.

However, whilst the user must take the consequences of his own decisions, he should have proper redress against organisations who supply product that is grossly defective (which does not exist at present). The Government should have a responsibility to look after its citizens by holding suppliers to account for negligent design of their products.

The citizen should also be able to take action against organisations that disclose personal information, as this could be seen as theft.

9. *What is the standing of UK research in this area?*

BCS would not wish to comment on this area.

Governance and Regulation

10. *How effective are initiatives on IT governance in reducing security threats?*

IT governance of itself is of little use to the citizen—even if the citizen knew about it and understood it much of current governance regulation is irrelevant to a home user. IT governance (or at least the security aspect thereof) is of value to organisations in achieving two objectives:

- bringing real discipline to IT departments; and
- ensuring that IT staff realise they are part of the organisation and there is a need to align their activities to the rest of the organisation.

The emphasis on introducing effective security into information systems, often as a result of regulatory pressure, has led to improvements in security in the larger organisations but has largely ignored small business, micro business and the consumer.

11. *How far do improvements in governance and regulation depend on international cooperation?*

International standards are key to a global economy. However, there are no international standards relating to the personal user.

Regulation is difficult because it is endlessly variable in detail. Regulation can make systems unnecessarily complex. Also software created in one country to their rules does not necessarily apply elsewhere even if it is sold as if it did.

International regulation would help provided the regulators in each country applied them in the same way, just as a wider implementation of ISO/IEC 27001 would help corporate and business users. It would also help business if general commercial regulatory activities did not appear to treat IT as a separate issue but made it clear that IT should be integrated into the business.

12. *Is the regulatory framework for Internet services adequate?*

Greater international co-operation on catching offenders and extradition treaty simplification in the case of computer crime would help more than regulation, from the citizen perspective. Computer Crime is international and the local ISP is often not in a position to deal with it, irrespective of regulation.

13. *What, if any, are the barriers to developing information security systems and standards and how can they be overcome?*

The major barrier is seen in the difficulty in reconciling the views of many different parties, which often requires a dilution of the required regulation. There are also different perceptions of personal responsibility, and a variable desire for a legislative solution to what can be seen as an issue of personal choice.

It is difficult to see, in practice, how international or even national standards would assist the consumer at the point he buys his broadband subscription, particularly if there is a cost penalty to adherence to standards which would make him choose a noncompliant supplier on cost grounds.

Crime Prevention

14. *How effective is Government crime prevention policy in this area? Are enforcement agencies adequately equipped to tackle these threats?*

The present legal structure is probably adequate, given that current changes are enacted. The Police are considerably under strength to address cyber crime, given that their computer experts are also involved on "higher" priorities (eg terrorism and pornography). The police would benefit if skilled people in organisations were able to present to them the necessary details for prosecutions in a form suitable for evidence However there is no public guidance as to how to do this in detail (the ACPO guidelines provide an overview). This hinders the public from assisting the police (and possibly reporting the crimes). The Police advice is that the

citizen reports all cybercrime to the local police station on paper. The effect of this is the people do not report the crimes, which leads to underreporting and is bad for governance generally. Also the citizen will often get a very poor impression of the Police if they try to do this.

15. *Is the legislative framework in UK criminal law adequate to meet the challenge of cybercrime?*

The framework is probably adequate in general, but theft of intellectual property is an area where the framework could be improved. White collar crime gets a low priority unless it involves huge sums of money.

16. *How effectively does the UK participate in international actions on cybercrime?*

The provisions of The European Convention seem to have been implemented as expected, and the UK would appear to play its part.

Annex 1

Input from BCS Education and Training Expert Panel:

This document has been drafted to inform the BCS response to the House of Lords Inquiry, and has been developed in consultation with members who all have a wide range of expertise in schools, HE and industry.

It has taken a focus on young people in school, but also out of school as all young people are encouraged by the education system to make greater use of the Internet and also they are major personal users of the Internet as "digital natives".

Defining the Problem

1. *What is the nature of the security threat to private individuals?*

Young people in and out of school use a whole range of devices and services to access the Internet to communicate with "friends", including net friends. The social networking phenomena have already emerged with students enetworking as an accepted core activity mixing chat, email, SMS and voice across mobile phones and computers. Young people do not fully understand the power of the Internet or of communication and can often think of the Internet as some sort of game that they wish to fully exploit.

Teachers expect children to have ready access to the Internet in and out of school to support and extend their learning and self development.

Parents trust the use of the Internet by their children as they cannot fully control access. Parents admit that students are in their rooms using the Internet and believe this to be a natural thing to do. Basically parents do not understand the power of the Internet. Young people change their use of technology and applications, such as games, at a faster rate than parents, generally leaving parents behind in their technical capabilities or understanding to control the actions of their children. The depth of understanding of internet applications, such as games, by parents is superficial compared to their children.

2. *What new threats and trends are emerging and how are they identified?*

The emergence of social networking and adoption by large numbers of young people.

The expectation that children will have a safe and secure online learning space accessible in school and out of school.

The rapid update of new online social environments such as MySpace and Bebo, as well as generic tools such as blogs and wikis where young people can exchange views and develop ideas, but can also leave themselves open to abuse, especially with the disclosure of personal information and forming of net friendships.

The cyber bullying of young people (and vulnerable adults) by their peers and strangers over which no one institution or law and order organisation can deal with.

Impersonation and the creation of (multiple) false identities by adults for grooming purposes leading to increased opportunities for virtual and physical abuse.

3. *What is the scale of the problem? How are security breaches affecting the individual user detected and recorded?*

All young people in the UK school system have increasing access to the fast and reliable Internet services in schools and are encouraged to use these services out of school to extend opportunities to access learning.

School systems should be set up with an appropriate accreditation of internet access (perhaps via BECTA) to provide for minimum standards, although schools are able to set differing standards for staff and children.

Schools are advised to establish and seek conformance to an Acceptable Use Policy and may install local monitoring software and manage access to specific sites as well, as generic types of sites, and follow up specific abuse allegations within their child protection regime. Some students have found ways round school security systems. The operation of esafety security systems can be seen as an overhead and limit the opportunity for innovation by staff.

The reporting of security breaches operates within frameworks established by Local Authorities and Regional Broadband Consortia as well as in schools. Reporting to appropriate authorities follows locally determined procedures, increasing in line with the guidelines offered by CEOP and BECTA.

As specific security and safety threats are dealt with in school, young people revert to open email and mobile phones out of school constraints.

Schools often focus on Internet security for young people overlooking the threats posed by staff to people in school and wider afield.

4. *How well do users understand the nature of the threat?*

School teaching and non-teaching staff often have a limited understanding of the nature of the threat or its pervasiveness, although schools are often aware and have formal policies in place—it is embedded practice that needs to be established.

Young people and school staff are generally confident they can look after themselves.

Tackling the Problem

5. *What can and should be done to provide greater computer security to private individuals? What, if any, are the potential concerns and tradeoffs?*

All schools should offer access to the Internet through accredited education ISPs. This may be seen as draconian; perhaps other controls can be established, such as relying on the inspection regime for maintained and independent schools. There is a balance to be achieved as a prescriptive regime in schools and other institutions means children will use other means of Internet access and use services outside of a context for safeguarding children.

School level filtering needs to be appropriate for the age, capabilities and maturation of the children, staff and community.

The continuous training of staff, children and the school community needs to be established.

Monitoring of staff needs to take place alongside children—it cannot be assumed that it is only children who will create the personal and network security threat.

All users to have a unique identity for monitoring purposes.

A greater understanding of the benefits and consequences of an increasingly diverse range of access mechanisms and applications to exploit the Internet.

It is likely that the greatest impact on computer security will not be through some technical means, but by focusing on user awareness and training so they become safe users.

6. *What is the level of public awareness of the threat to computer security and how effective are current initiatives in changing attitudes and raising that awareness?*

The education "public" is generally not well informed—a few headlines grab the attention—paedophiles and social web sites current—cyber bullying, but on the whole it is limited.

Provision of education ISP accreditation is affecting the technical provision but user awareness and understanding still low priority; LAs are responding, but the wider ISP marketplace is still relying on the IWF lists and users.

7. *What factors may prevent private individuals from following appropriate security practices?*

Current filtering standards apply over a wide range of situations. However, there can be considerable differences between a person being in school and their being out of one. The general lack of understanding by parents regarding the nature of the controls that can be applied to risk is also an obstacle to improving the current situation.

There is a need for different levels of security when a child is in school from when they are in the safety of their home.

8. *What role does software and hardware design play in reducing the risk posed by security breaches? How much attention is paid to security in the design of new computerbased products?*

Education tends to include security and personal safety as high priorities which works well on school sites, however off site and in the home the situation is more problematic, especially for family computers used by adults and children.

9. *Who should be responsible for ensuring effective protection from current and emerging threats?*

National agencies and key vendors have a role in intelligence and keeping users aware of the changing nature of threats and prevention steps.

Education, so that young people know how to deal with and assess information and contacts on the internet and take appropriate precautions.

Parents through the rules and procedures they apply at home with the support from ISPs and other IT service providers.

10. *What is the standing of UK research in this area?*

The emergence of national education systems using the Internet has lead to the setting of standards—not aware of any research.

The Cyberspace Research Unit at the University of Central Lancashire[1] has a research focus and has developed web-based materials.

Governance and Regulation

11. *How effective are initiatives on IT governance in reducing security threats?*

The role of BECTA in defining standards has assisted in schools although the majority of schools still do not have a BECTA accredited supplier and even when they do they can override the accredited standards.

The role of BECTA is not fully accepted by schools and the ISP marketplace.
Standards outside of schools are subject to the vagaries of the marketplace and the selected ISP accessed in the home and at other sites.

The requirements for school level governance are ambiguous and can lead schools to believe they can self govern; a few can, but the majority who make such claims appear not have effective systems.

12. *How far do improvements in governance and regulation depend on international cooperation?*

Essential, but also needs to be sensitive to local contexts.

13. *Is the regulatory framework for Internet services adequate?*

No.

[1] http://www.uclan.ac.uk/host/cru/

14. *What, if any, are the barriers to developing information security systems and standards and how can they be overcome?*

The expectation that all ISPs are the same and that the user should determine what is appropriate in terms of access and use.

Crime Prevention

15. *How effective is Government crime prevention policy in this area? Are enforcement agencies adequately equipped to tackle these threats?*

CEOP are in their infancy but are already making a significant difference in raising the profile of esafety and ensuring training becomes more effective.

16. *Is the legislative framework in UK criminal law adequate to meet the challenge of cybercrime?*

No comment.

17. *How effectively does the UK participate in international actions on cybercrime?*

No comment.

October 2006

Memorandum by BT

Introduction

1. The Committee's inquiry is welcomed as a means of taking stock of where we are on this important issue. The Internet continues to grow in importance for individuals as well as businesses. Unfortunately, it is a sad fact of life that BT and others, including individuals, need to spend considerable time and effort in devising ways to protect themselves, their customers, their customers' information, and their assets from fraudsters and pranksters.

2. As in so many similar situations, as countermeasures develop so does the sophistication of those intent on causing problems. It is a constant battle to stay ahead that needs dedicated resources and a co-operative approach between individuals, industry and Government.

3. However, it is important to retain a sense of proportion. Existing laws are almost certainly adequate to deal with most of the issues that arise—there is very little that is actually new here, it is mainly just that today's electronic communication channels offer a different way for the issues to come to the fore. In any event, companies such as BT are working very hard to implement protective measures and are introducing new services, some applying automatically and some to be used by customers if they wish, that provide increasingly sophisticated protection. We are working both to protect our own end consumers and with other businesses who use our services and need themselves to help their customers.

4. Raising awareness of the issues leads to greater understanding by customers about what can be done to protect themselves, but this is an ongoing process. For example, there is plenty of advice on how to spot scam emails apparently offering good deals, amazing returns, cash and so on—all if you provide bank or other personal details. A measure of commonsense goes a long way too. However, whilst it may be obvious to most people that anything that seems too good to be true probably is, there seem to be lots of people who can be taken in when faced with such "amazing" offers.

5. In this response we provide comments on the specific questions posed in the questionnaire as well as a summary of some recent research into the issues surrounding trust, security and privacy in the electronic world.

Defining the Problem

What is the nature of the security threat to private individuals? What new threats and trends are emerging and how are they identified?

6. Most of the issues considered to be "threats" in the online world are actually just current manifestations of existing problems as seen through the medium of electronic communication. People need to be aware of potential threats, but to keep them in proportion. They need to take commonsense precautions, and take advantage of protection services, some automatic, some that must be applied, that are offered by companies such as BT.

7. There are three main areas of concern for private individuals relating to Internet security:

— online fraud, including identity crime;

— viruses, trojans and other malicious attacks; and

— child safety.

8. Impersonating someone else was an issue long before the advent of electronic communication. Gathering personal information about another individual is not something that can only happen through the Internet but, nevertheless, identity crime, as it is known, is a growing issue. In February 2006 BT published an Internet security report[2] on Online Identity Theft, written in conjunction with CPP, Get Safe Online, Lloyds TSB, Metropolitan Police and Yahoo! The report highlighted the growth of online threats and included advice on protecting identity and where to go for advice or help if problems arise.

9. BT has recently added Identity Theft Protection[3] to the other security measures available on its consumer broadband product BT Total Broadband.

10. Viruses, trojans, worms, spam and botnets[4] are still the most likely way in which online security will be breached. BT is committed to providing the best possible protection for its customers and to do this BT not only offers a range of protection in the network but also a wide range of security features are provided as part of the email, narrowband and broadband ISP service to UK consumers.

11. As well as BT and others providing security features, and individuals taking responsibility, companies offering online services work with each other and with Government on various initiatives to deal with these problems. For example, as well as the standard anti-virus and firewall products we provide, we are also working with anti-spam and anti-botnet groups led from the UK (ISP and DTI led groups) and international groups such as the OECD. We are members of the International Botnet Task Force. In all cases we are working with law enforcement agencies.

12. On Child Safety there are various initiatives designed to make for a safer online environment, recognising that children are less experienced in the ways of the world and may have a propensity to divulge more information about themselves to strangers than they ought. This, of course, is an issue much wider than just in the online environment. BT has led the way in trying to deal with child pornography through its Cleanfeed project,[5] which prevents access to sites identified by the Internet Watch Foundation as illegal. We are one of the sponsors of Get Safe Online, which provides advice on Internet security. Our own BT Broadband services offer inclusive online security features, including Parental Controls as well as anti-virus and firewall products.

What is the scale of the problem? How are security breaches affecting the individual user detected and recorded?

13. It is not possible to provide a meaningful answer to this question. The February 2006 report mentioned above contains some research data but this does not pretend to be definitive nor does it cover all issues that might be thought to represent what is covered by the term "security breaches". Individuals will become aware of matters relating to, for example, viruses or identity, at different stages, depending on the nature of the issue and their own online behaviour patterns.

[2] http://www.btplc.com/onlineidtheft/onlineidtheft.pdf

[3] Free of charge on BT Total Broadband options 2 and 3.

[4] The term "virus" is used to cover all kinds of malicious or undesirable software. A "worm" is like a virus in that it replicates itself but it does so without attaching itself to a host program. A "trojan" is an apparently useful program containing hidden functions that can exploit the privileges of the user to do things the user did not intend. "Spam" refers to electronic junk mail or junk newsgroup postings. A "botnet" is a term for number of Internet computers that, although their owners are unaware of it, have been set up to forward transmissions (including spam or viruses) to other computers on the Internet.

[5] A filter which blocks child abuse sites. It is available to all ISPs.

How well do users understand the nature of the threat?

14. Trustguide[6] is a collaborative project between BT Group and HP Labs, in partnership with the University of Plymouth's Network Research Group, continues the dialogue that began with the Foresight Cyber Trust and Crime Prevention project focused on building a safer cyber world. Trustguide was concerned with exploring issues of trust, security and privacy in ICT based applications and services via a series of workshops and discussion groups that covered as broad and appropriate a spectrum of the UK's citizens as the scope of the project allowed. The aim of the project was to use this dialogue and its outputs to establish recommendations and guidelines for the research, development and delivery of trustworthy ICT and to inform the policymaking processes used by government, industry and other key organisations.

15. In summary, the report suggests that consumers have a basic level of understanding that threats exist and that they need to protect themselves against them. The depth of that knowledge is less obvious; while people were confident in using appropriate terms, further investigation revealed little evidence of in depth appreciation and awareness of the dangers.

Tackling the Problem

What can and should be done to provide greater computer security to private individuals? What, if any, are the potential concerns and trade-offs?

16. Internet security is both a product issue and a consumer concern. Amongst other things, consumers should:

- understand the risks and safeguards available;
- ensure firewall, anti-virus and anti-spyware software are installed;
- keep these protections up to date;
- keep their computer operating systems up to date;
- protect personal and financial details; and
- set up parental controls where children are computer users and move the computer to a family room.

17. To supplement the actions consumers should be taking themselves in terms of managing protection software, ISPs can take additional measures on their behalf. For example on 12 October, BT announced it was implementing a new spam detection system "Spam Buster", which not only tracks down "professional" spam emanating from the BT network but also protects individual PCs against being hijacked to produce more spam.

18. There is also an issue for hardware and software development in that products are often released to the market before being fully checked for flaws, which means that many software vulnerabilities are only discovered once a product is in live use. Greater checking beforehand could, of course, lead to more costly products and later market availability, so there is a balance to be struck.

What is the level of public awareness of the threat to computer security and how effective are current initiatives in changing attitudes and raising that awareness?

19. See the Trustguide report for awareness levels. Set against a background of plentiful advice from ISPs, government, campaigns of various sorts, it is clear that changing attitudes and awareness is a matter of education—and education from an early age is as important as "educating" older sections of the population through advertising and advice.

What factors may prevent private individuals from following appropriate security practices?

20. There may be a lack of awareness of what is available and what can be done. There may be a confidence issue—how to get the best from the services and software possibilities on offer? Even with awareness and competence, however, people do not always do the "right" thing—we know we shouldn't smoke, or drink and drive, or break the speed limit, or cross the road without looking, etc. But people do all of these things and there is nothing special about them not taking all the precautions available online.

[6] http://www.trustguide.org.uk/Trustguide%20-%20Final%20Report.pdf

What role do software and hardware design play in reducing the risk posed by security breaches? How much attention is paid to security in the design of new computer-based products?

21. Some security should be built into operating systems or hardware and enabled by default. A high degree of automation will avoid customers having to configure services themselves, which will reduce the potential security risk. An example of hardware security is contained in the BT Home Hub. It contains Firewall and Intruder Protection software which are switched on as the default setting. Where customers need to proactively download or activate new protection software, ISPs in general are trying to make this simpler.

Who should be responsible for ensuring effective protection from current and emerging threats?

22. ISPs, software vendors, network operators, government, educators and customers all have a part to play.

What is the standing of UK research in this area?

23. BT is actively engaged in a wide-range of research and innovation activities, engaging with world-leading teams around the world. Other UK companies are similarly engaged.

24. As is common in Internet-related activities, sources of innovation are globally distributed. Investment in research in this area probably reflects the patterns indicated in recent R&D surveys, ie UK spending in terms of a percentage of GDP is higher than in some EU countries, but is lower than the USA. The rate of research spending, including the development of post-graduate researchers, in the Far East is rising quickly. Overall, surveys indicate that the quality of UK research is high, but there is a need to ensure that gaps in investment in research between the UK and other countries and regions are closed.

Governance and Regulation

How effective are initiatives on IT governance in reducing security threats?

How far do improvements in governance and regulation depend on international co-operation?

Is the regulatory framework for Internet services adequate?

25. Increasing usage of ICT and the Internet has led to an increase in the perpetration and propagation of security issues with a cross-border element. A corresponding increase in focus on developing effective mutual co-operation between relevant agencies to investigate and pursue harmful cross-border activities is needed, together with increased resources to deliver results.

26. However, rapid progress is an unrealistic expectation, given delicate issues of national sovereignty, different priorities of governments and the absence of uniform global standards in this evolving area. Continuing dialogue and exchange of best practice would seem to be the appropriate model to cultivate a shared understanding of the issues and challenges and the motivation to provide effective mutual assistance. The example of the recent successful prosecution and harsh sentences handed out in Russia to perpetrators of a Denial of Service attack illustrates that progress is being made.[7]

27. We believe it is for users and service providers alike to take security measures, rather than for regulation or law to be relied upon to drive this. Security is a matter of great importance and service providers in a competitive market, such as we have in the UK, are driven by the demands of customers and by the pressure from other providers to offer and provide ever more sophisticated and powerful security services in order to maintain their competitiveness.

What, if any, are the barriers to developing information security systems and standards and how can they be overcome?

28. Money may be considered to be one barrier but there are organisations, like BT, who implement security initiatives such as Cleanfeed without making them commercial investments. They are seen as part of our corporate responsibility to our customers and beyond.

[7] http://www.kommersant.com/page.asp?id=709912 "Eight Years for Extorting Millions" The Balakov City Court, Saratov region, has sentenced to eight years in colony with a strict regime and 100,000-ruble penalty each of three hackers of Russia accused of extortion, causing material damage and establishing and applying hostile software. Investigating the case of Russian hackers that used to blackmail British companies lasted for a year.

29. Indeed, there are strong incentives to invest in security issues in order to build and maintain a good reputation, and to match what others are offering, even if such investments are not immediately seen as commercial propositions.

Crime Prevention

How effective is Government crime prevention policy in this area? Are enforcement agencies adequately equipped to tackle these threats?

Is the legislative framework in UK criminal law adequate to meet the challenge of cyber-crime?

30. As stated earlier, we believe the existing legal and regulatory provisions to be adequate for dealing with issues arising from the use of electronic communication services. There must be a sense of proportion when considering "problems" and potential solutions. For example, not all spam is criminal or a security issue, and not all mass-mailings are "wrong".

How effectively does the UK participate in international actions on cyber-crime?

31. The Internet operates across borders and so we need international co-operation to manage issues around its security. The UK has taken a very sensible decision to foster cross-border co-operation rather than looking at issues in national isolation.

32. The UK Government, regulatory and law enforcement authorities are involved in partnership with industry (including BT) in a broad range of initiatives in the OECD, ASEM (Asia-Europe Meeting) and EU. The Virtual Global Taskforce (police forces from around the world working together to fight online child abuse) is one such initiative in which initially bilateral co-operations are being successfully developed into a broader matrix of co-operation with agencies around the world.

33. We believe that the UK has a key role in these initiatives as a consistent, balanced and credible "voice of reason". This is made possible by the shared understanding in the UK across all stakeholders that:

- dealing with personal Internet security is a risk-management issue in which there is shared responsibility;
- personal behaviour is ultimately more important in managing the risks than a purely technical approach;
- many features which impact on security are not intrinsically and unequivocally malign and damaging, but the context for their use may lead to negative outcomes;
- technology and behaviour continue to evolve; and
- considerable variation exists between different countries in their traditions and cultural approach to security and protection issues and widespread usage of ICT (including the Internet) exacerbates the challenges of reconciling these different approaches.

34. This means that the UK brings to such international actions a pragmatic, nuanced and holistic approach that recognises that rushing into legal and regulatory interventions is inappropriate and has real potential to create unwanted, unintended consequences.

35. BT is an active supporter of both national and international co-operative action. As we move into the implementation of our 21st Century Network we will continue to secure our Networks and work with various organisations to stay one step ahead of problems as far as we can. For example, BT is currently involved in several initiatives, such as:

- G8 Working group on strengthening partnerships within Government and Businesses;
- International Botnet Task Force (Microsoft and LEA initiative to combat organised crime and protect the public);
- GIAIS (Global Internet Alliance for Information Security. A Microsoft run programme to help ISPs and Corporates protect their customers);
- FIRST (Forum of Incident Response and Security Teams—a trusted group of over 130 Blue Chip companies that share information on Internet Security);

— TF CSIRT (a trusted European forum of Computer Security Incident Response Teams that have pressed the EU into funding training legal handbooks and several other projects. They also share information and provide and early warning network); and

— ETIS (the global IT Forum for Telecommunications).

October 2006

Letter from Duncan Campbell

I work as a forensic scientific expert witness in criminal cases. I have been instructed in more than 20 Operation Ore prosecutions, and have advised in many similar cases. I am a Law Society registered expert witness.

I was surprised to read testimony given to the Committee on 11 January 2007.

Lord Erroll put a number of informed questions to your witnesses Mr Gamble and Ms Girling of CEOP in respect of Operation Ore. In particular, he asked "Is there possibly going to be a problem with the amount of credit card theft—identity theft as people have re-named it—that is going on at the moment?"
Mr Gamble replied "We never prosecute someone simply on the basis of their credit card being used". (Q 221)

I am unable to understand how Mr Gamble, who has led these enquiries for five years, could have so mis-stated matters to the Committee. There are, and continue to be, many prosecutions of this type. Most Operation Ore prosecutions are and were of this nature. Such cases involve charges of "incitement" only, and are based solely on data and records recovered in 1999 from a US Internet company. There is no collateral information to support these "incitement" charges. Indeed, the charges were devised and applied precisely because there was no other information or evidence. They are used systematically, when police forensic examination of a suspect's seized computers show no evidence of child pornography, nor of any interest in or attempts to acquire such material.

I was, further, at a loss to understand why Ms Girling did not seek to correct her colleague's omisison when appearing before the Committee. She cannot in my direct experience be in any doubt about the position. She personally has attended a number of such trials in my presence, and is scheduled to attend many more, in each of which defendants continued to be prosecuted and to face jail sentences, loss of family and career, and the stigma of a Sexual Offenders Register entry, solely on the basis of their credit card data and personal information having been used by third parties for financial gain in 1998 and 1999.

Ms Girling and I both attended Stafford Crown Court in January 2006 for three Operation Ore incitement cases. On 20 January 2006, His Honour Judge Mitchell asked how many cases of this type were still outstanding. Through the prosecuting advocate, Ms Girling replied that there were two thousand such cases.

Within a few hours of the evidence to the Committee being published, I received e-mails and other communications from current and past defendants in these matters. These correspondants expressed outrage at what had been said to the Committee, because they knew from personal experience that the statements made were wrong. Several of them offered to give evidence if desired, or even to appear before the Committee and display the indictments they faced or face, as plain evidence of the correct facts.

I understand that your current inquiry is not focused in the shortcomings of Operation Ore. However I presume you are concerned about the truthfulness of witnesses who appear before you. I attach two recent judgements [not printed]. *R v Grout* is a case in which the defendant was a victim of credit card identity theft, and was acquitted after precisely the kind of prosecution whose existence was denied to you by Mr Gamble. The second is *R v Chief Constable of A ex parte C*, which documents many of the abuses of legal and police procedure with which Operation Ore has unfortunately been contaminated. I am aware of many other similar cases.

These cases raise broader issues of relevance to your inquiry than the possible misconduct of a particular police unit. These issues could include the police failure to understand the nature of the Internet, the inadequacy of police computer forensic resources, and the inappropriate use of resources that should have been deployed against Internet financial crime and Internet organised terrorism. These management failings contribute directly to the poor personal security enjoyed online by UK citizens.

I myself would be happy to attend before you and provide evidence.

10 February 2007

Letter from Duncan Campbell

Thank you again for your email of 16 April 2007 concerning questions raised by the Committee with Mr James Gamble of CEOP.

I strongly believe in public enquiry, public accountability, and fully support the principle that material before and procedings of the Committee should ordinarily be public and published.

Mr Gamble writes on 23 March 2007 to ask you to forward "evidence in your possession or the letter you have received to better inform our process". This appears odd. Surely the purpose of such correspondence is for him to better inform the Committee? His letter could suggest that his aim is to place the Committee's sources and methods under investigation. He omits any undertaking to respond in the correct way to the Committee.

The letter therefore raises misgivings in my mind. I hope it will not seem a distraction if I briefly explain these.

My misgivings are strengthened by a recent professional experience when I attended before the Recorder of Belfast in February. I prepared for the Recorder, through Queen's Counsel, a draft order listing details from CEOP held files in Operation Ore which were needed to establish the scale of Internet credit card theft and fraud that was evidence in computer records held, but never produced, by CEOP and the Crown Prosecution Service.

When the draft order as produced, CEOP staff present in Court directed PSNI officers to seize the document, and to withhold it from the Court as "evidence". They refused to obey a specific order from the Judge to surrender it. I personally was then also threatened by being advised several times that I should be cautioned, although it was not suggested what alleged offence I had committed in drafting a request for the Court to consider.

This remarkable episode was brought to an end when the Recorder arranged for a second Crown Court Judge to attend his Court potentially so as to punish the officers if they continued their contempt. The document was then surrendered. The Recorder is now to hear an abuse of process application against the prosecution for threatening a witness.

It came to light on the same occasion that a team of CEOP officers had spent at least 18 months on an intrusive personal investigation into myself, collecting documents as bizarre and widespread as student letters written in 1974 and irrelevant postings from Internet conspiracy sites. As part of these investigations, they have several times instructed prosecutors to falsely accuse me of fraud. To date, no judge has listened to the allegations. CEOP prepared and handed in a 50 page dossier concerning me at the start of the Belfast matter, but were not able to present it when their own misconduct became the central matter of concern to the Court.

This unusual approach to evidence, witnesses and justice has persisted through the course of Operation Ore, specifically in relation to the cases of allged credit card use for incitement (about which I first wrote to the Committee).

I have described in a 2005 computer article how Internet evidence used generally in Operation Ore was founded on falsehoods.[8] In a second article to be published tomorrow by *PC Pro* magazine and in abridged form in *The Guardian,*[9] I describe how CEOP and the Crown Prosecution Service have withheld critical and important evidence from the Courts and defendants throughout the course of Operation Ore. In particular, the evidence withheld shows conclusively that Landslide Inc (the Texas pornography provider) was in possession of, and the vehicle for the re-use of, credit card information stolen by hacking from commercial companies in the same manner as the current TK Maxx issue in Britain and the United States.

The third arm of CEOP's approach in Operation Ore cases has been to seek to exclude, or otherwise obstruct, investigate and attack defence witnesses who have raised critical questions about their evidence. CEOP have demanded the right to approve defence witnesses and to control the selection of such evidence as they see. Although attempts to attack me personally have been rebuffed (several times), a second and very experienced defence computer expert, a Mr James Bates, has been subject to harsher difficulties over a three year period and indeed has been charged by CEOP with alleged fraud.

I would very much hope that the reason Mr Gamble replied to the Committee in the terms he did is not because he inteneds to ignore the issue the Committee raised about his own evidence and was instead seeking to add another document to the CEOP "enemies list" dossier.

Having set out my misgivings, I would return to the principles in my second paragraph. I agree that my letter of 10 February 2007—and indeed all correspondence (other than my full personal address and phone numbers)—can be regarded as Parliamentary papers, and be published with the Committee's report(s). The

[8] "Operation Ore exposed" *PC Pro,* August 2005.
[9] "Sex, lies and videotape" *PC Pro,* June 2007.

corollary, on which I would insist, is that if my letter is sent to Mr Gamble privately, he is advised at the same time that it and his response(s) will be public and published, in the same way as his original evidence.

I reaffirm that I am willing fully to assist the Committee by providing oral or other evidence. If it were the Committee's wish to seek common understanding of the matter by asking for the joint attendance of myself with Mr Gamble and/or other witnesses, I would be happy to agree. I have previously attended as a witness at Parliamentary Committee hearings, including a session of the House of Commons Health Committee where I and a UK tobacco control advocate were questioned together with the Chairman and Deputy Chairman of British American Tobacco.

If I may add an afterthought within the Committee's current remit, it would be that by far the largest part of my current work as an expert witness in computers and the Internet is for radical Islamist inspired terrorism cases. It is common knowledge that the Internet supports many networks circulating radicalising and extreme materials, including voluminous manuals on military and terrorism methods. The types of problems and events I mention do not affect such cases and trials, nor do they appear in other Internet paedophilia cases. In my experience, they have occurred solely in the context of Operation Ore.

18 April 2007

Memorandum by East Midlands Broadband Consortium

The East Midlands Broadband Consortium (embc) is one of the 10 Regional Broadband Consortia (RBC) formed as a result of the DfES Regional Broadband initiative. Embc is a collaboration between the nine East Midlands Local Authorities, and currently provides connectivity to over 2,100 schools in the East Mildands. This response is given from an education point of view, particularly in the context of child safety.

Defining the Problem

What is the nature of the security threat to private individuals? What new threats and trends are emerging and how are they identified?

1. Online technologies such social networking sites, email, chatrooms etc are increasingly popular and extremely widely used by children and young people.

2. Such technologies allow individuals to hide or disguise their identities. Paedophiles and other predators are able to access children under false pretences, for the purpose of grooming or other illegal activity. Such individuals are able to find or elicit personal information that helps them in their illegal activities. This provides a means of access to children and young people that has not previously existed and is therefore a new threat in terms of child safety.

3. CEOP, police forces and other organisations concerned with child safety have noted increasingly sophisticated use by paedophiles of online environments to access children and young people, with little or nothing in the way of vetting to ensure they are who they say they are.

4. Another increasing trend is that of cyberbullying, where children and young people are subjected to extremely disturbing forms of bullying and public humiliation, not just within their circle of acquaintances but also online for viewing by anyone with a connection to the internet.

5. Parents do not generally understand the nature or extent of potential threats, and therefore are not in a position to teach their children how to keep safe.

6. Parents also tend not to understand enough about how the technology works to be able to implement suitable monitoring and control measures.

What is the scale of the problem? How are security breaches affecting the individual user detected and recorded?

7. In education terms, the expectation is increasingly that children and young people will have ready access to the internet in and out of school to support and extend their learning and self development. The expectation detailed in the DfES e-strategy is that children will have a safe and secure online learning space accessible in school and out of school. In school, it is possible to offer safe and secure access to the Internet where the connection is provided by an RBC such as embc. However, in the home the level of safety and security is determined by the child's own level of understanding and that of his or her parents, which may be very limited.

8. Children and young people expect to be able to use a range of online technologies, in particular various forms of social networking, in order to keep in touch with both real and "virtual" friends. Use of such technologies is increasingly the norm, and hence the potential threat affects the vast majority of children.

9. Detection and recording can take place using monitoring software and by managing access to specific sites. However, this is extremely difficult to do in the home if the users are not aware of the technology available to do this, or how to implement it, in order to keep themselves safe. Such safeguards would generally fall to the parents, who on the whole are less well informed in these matters than their children.

10. In terms of personal safety however, it is currently impossible for an individual to know whether the person they are "talking" to online is who they say they are.

11. CEOP is assisting with increased emphasis on e-safety, has launched a campaign for young people to help them better understand the dangers and be in a better position to avoid them. Organisations such as Childnet International are also attempting to help with information for parents. However, reaching the intended audiences is difficult.

How well do users understand the nature of the threat?

12. General understanding is currently poor. Both adults and children are not well enough aware of the strategies used by pedophiles or other individuals with intent to harm. There is a lack of understanding of the how the various pieces of information available online through personal profiles, blogs, podcasts etc can be used by criminals to support their activities. Young people are generally confident they can look after themselves, but do not always understand the consequences (both short term and long term) of their social networking, eg the publishing blogs or images which give out personal information and which may impact on their personal safety in the short term, or simply be embarrassing to them in a personal or professional context in later years.

13. In addition, parents may be unaware of the activities their children are taking part in (eg inappropriate use of web cams in bedrooms) or may not understand the implications and possible consequences of such activities.

Tackling the Problem

What can and should be done to provide greater computer security to private individuals? What, if any, are the potential concerns and trade-offs?

14. All schools should offer access to the internet through accredited education ISPs. Filtering levels in school need to be appropriate for the age and maturation of the children.

15. A greater emphasis needs to be placed on training and raising awareness of the dangers and how to avoid them—for children, parents and school staff. This is particularly crucial for children and young people as very often they will have access in the home to sites and facilities that will be blocked within school. They need to understand the reasons why these are blocked and how to keep themselves safe when they do have access to them.

What is the level of public awareness of the threat to computer security and how effective are current initiatives in changing attitudes and raising that awareness?

16. Public awareness is generally not good. A few headlines grab the attention eg paedophiles, pornography in social web sites, cyber bullying, but little true understanding of how the sites may pose dangers, or what can be done to prevent problems occurring.

17. CEOP and Childnet have recently launched safety initiatives, but it is too early to comment on their effectiveness.

What factors may prevent private individuals from following appropriate security practices?

18. Lack of understanding of the nature of the potential dangers and of the controls that can be applied to risks. This applies both the technological and the cultural aspects. In many cases individuals do not understand what is available to ensure filtering and other safeguards, or how to implement it. There is also a lack of understanding, particularly amongst children and young people about how the information they disclose to the world online might be used by others and the consequences this may have.

What role do software and hardware design play in reducing the risk posed by security breaches? How much attention is paid to security in the design of new computer-based products?

19. Easy-to-use and install software is a key aspect of enabling personal safety online. In many cases individuals will not even be aware that software is available to help with the security or safety issues they may be concerned about.

20. Out of school and in the home the situation is more problematic, especially for family computers used by adults and children.

Who should be responsible for ensuring effective protection from current and emerging threats?

21. National agencies and key vendors have a role in intelligence and keeping users aware of the changing nature of threats and prevention steps.

22. Providers of online facilities such as social networking that provide access to individual and personal information also bear a responsibility for ensuring that the content they host is appropriate and for educating their users in the potential dangers.

23. Children's services should be providing a unified approach to the advice it gives to children and young people.

What is the standing of UK research in this area?

24. The emergence of national education systems using the internet has led to setting of standards—we are not aware of research in this area.

Governance and Regulation

How effective are initiatives on IT governance in reducing security threats?

25. The role of Becta in defining standards has assisted in schools although majority of schools still do not have an accredited Becta supplier and even when they do they can override the accredited standards.

26. Standards outside of schools are subject to the vagaries of the marketplace and the selected ISP accessed in the home and at other sites.

How far do improvements in governance and regulation depend on international co-operation?

27. This is essential, particularly with regards to child safety, but also needs to be sensitive to local contexts.

Is the regulatory framework for Internet services adequate?

28. No.

What, if any, are the barriers to developing information security systems and standards and how can they be overcome?

29. The expectation that all ISPs are the same and that the user should determine what is appropriate in terms of access and use.

Crime Prevention

How effective is Government crime prevention policy in this area? Are enforcement agencies adequately equipped to tackle these threats?

30. CEOP is in early days but is already making a significant difference in raising the profile of e-safety and ensuring training becomes more effective.

Is the legislative framework in UK criminal law adequate to meet the challenge of cyber-crime?

31. Not known.

How effectively does the UK participate in international actions on cyber-crime?

32. Not known.

Memorandum by Eurim

1. Who Are We?

EURIM is a UK based Parliament-Industry Group. It brings together politicians, industry and officials to secure action on issues not already well addressed elsewhere. Debate over the need to greatly improve the safety and security of the Internet goes back more than a decade to when it began being used for business and consumer purposes. There is confusion and conflict over objectives as well as what is practical or economic and the responsibility and ability to take effective action are fragmented. EURIM welcomes the focus of this inquiry on addressing the needs of the most vulnerable, believes it asks the right questions.

This response is structured around those questions and is intended to provide an introduction to the issues, using material and recommendations already on file and agreed. We have asked our members to respond direct to the Committee in more detail, especially on areas where there is disagreement between industry players. We are also consulting them on additional recommendations where we believe there might be pan-industry agreement and will report the results separately. There is much additional material on www.eurim.org.uk.

2. Defining the Problem

You will receive many definitions of the "problem" and we believe these reflect an over-arching failure to connect the debate over the promotion of the Internet and the many benefits that it brings with that on the need to improve safety and security. Even when the same organisations are involved in both debates, they are commonly represented by different individuals, from different departments, with different terms of reference.

The debates should be seen as two sides of the same coin. Promoting confident, secure and socially inclusive access to the global information society requires joined up thinking. It also needs to be seen in context, as part of a wider debate on the need to promote also the safe and secure use of the Internet by business and government—including along supply chains and across markets. One aspect of this is the need for government itself to follow good practice in ensuring that its own systems are both adequately secure and also accessible and "user-friendly".

2.1 *What is the nature of the security threat to private individuals? What new threats and trends are emerging and how are they identified?*

The Internet is an open-access network of networks with security and authentication added according to the expertise and budgets of those paying for access. It is a great force for good, but like all great forces it can also be misused. Over 10% of mankind is now on line, but so are at least 10% of the world's literate criminals. The scale and sophistication of computer-assisted malpractice is increasing dramatically, with the Internet used to automate the identification and exploitation of prospective victims over the converging media (fixed and mobile, voice, data and video). So too is the use of the Internet and mobile communications at every level of anti-social behaviour. From teenage gangs to international terrorism, from text-bullying, on-line paedophile grooming and cyber-stalking through impersonation, fraud and extortion to sophisticated attacks on critical infrastructures (especially payment systems), delinquents and criminals appear well ahead of law enforcement in their use of new technology.

Emerging threats are commonly identified first by the customer protection and security teams of the main service providers (eg BT or Vodafone), e-commerce players (eg Amazon or e-Bay) and those who provide them with attack monitoring and traffic filtering services (eg Symantec or Mark Monitor). Government Regulators and Law Enforcement commonly lack perspective because they are overwhelmed by *ad hoc* reports. They need to make better arrangements with the private sector to accept collated inputs and then to act on reports of situations where individuals are at personal risk. Recent progress with regard to global co-operation on child

protection indicates how this might be progressed in other areas as well. Where individual users or customers identify a problem they are often unable to alert others quickly because of the problems identified in the next paragraph.

2.2 *What is the scale of the problem? How are security breaches affecting the individual user detected and recorded?*

The near impossibility of reporting individual incidents to someone who will accept the report, let alone help the victim obtain redress, undermines the chance of acting on "early warnings" and it also means the actual impact is unknown. However, the incidence of phishing and spam and the growing publicity for the consequences of fraud and abuse, is clearly affecting confidence in the Internet as a safe place to do business, let alone for our children to learn and play. A consequence is regular proposals for new reporting mechanisms to replace those that are not working. Public pressure for Government(s) to "do something" leads directly to proposals for legislation or regulation—but such processes take a long time and often end up being inadequately targeted. Most such proposals do not address the root causes of failure. In addition, no one has an incentive to report incidents merely for statistical purposes or to accept reports to which they can respond only by admitting ignorance or inability to help.

Individual phishing attacks may not justify the use of scarce investigative resource but analyses by global private sector monitoring organisations indicate that a large proportion of malpractice originates from a relatively small number of loose-knit criminal networks, many of whose members could be tracked, traced, removed and blacklisted ("the e-death penalty") by the main communications operators for breach of service conditions. There is a need to bring the current proliferation of fragmented local and national reporting operations together into international reporting networks that cross public-private boundaries and to collate and route information to those who are in a position to take action.

Proposals for new reporting agencies should be replaced by proposals for secure information exchange, including internationally. These should involve the abuse@ teams of the communications service providers and reputable private sector monitoring operations to enable (for example) collated analysis of phishing and malware incidents to be passed rapidly to those able to block attacks and blacklist the perpetrators for breach of conditions of service. There is also a need to consider reporting structures for the actions then taken by the latter.

2.3 *How well do users understand the nature of the threat?*

Surveys after the Get Safe Online Campaign and the recent Ofcom Media Literacy Survey indicate a high level of awareness of those risks for which vendors are already promoting "solutions" accompanied by a lack of confidence in respondents' ability to understand or use the tools on offer or to identify anyone competent and trustworthy to help them at a price they can afford. The website of the Identity Theft Assistance Group[10] (funded by US financial services players like Bank of America, Bank of New York and Citigroup) carries a report saying that "More than two thirds of the American public has lost confidence in the handling of their personal information", one in four web users had stopped shopping on-line because of perceived security risks, more than half no longer gave personal information over the net and 6% had changed banks to reduce their risk of becoming a victim of identity theft. However, over 60% still trusted their banks compared to under 30% who trusted on-line retailers. A more recent UK survey indicated significantly lower levels of trust with only 37% trusting their banks and only 17% trusting government.

Well-publicised stories of the theft of files of personal details from both public and private sector to aid impersonation and fraud and the current plagues of phishing, vishing (semi-automated phone calls using voice over IP) and spam mean that consumer trust in on-line transactions is increasingly fragile and needs reinforcement. Given the growing use of the Internet for consumer and political research of all types, it is surprising how little consumer research has been done into what Internet service providers' customers expect, would like, or are willing to pay for. There is a common attitude that the Internet is too complicated for customers to understand and decisions should therefore be left to industry or government, advised by academic experts. But many consumers no more wish to receive anonymous and unsolicited e-mails than they wish to receive anonymous letters or unsolicited phone calls. Why should they not be able to ask their Internet Service provider to automatically return these to sender? (see 3.1 below).

Awareness of those threats from wireless interception and from that spyware for which low cost solutions are not readily available or promoted, appears largely confined to security professionals. Many security breaches resulting from the use of insecure Bluetooth mobiles, unencrypted WiFi hot spots and shared ADSL systems remain unknown until long after the captured passwords and account or personal details have been used.

[10] www.identitytheftassitance.org

3. Tackling the Problem

3.1 *What can and should be done to provide greater computer security to private individuals? What, if any, are the potential concerns and trade-offs?*

Until 2005 one of the priorities of the Internet Engineering Task Force, (IETF), was to retrofit quality of service and security to a previously open access, "best efforts", academic network before the consumer backlash against variability of service and criminal abuse brought the technology into disrepute. The security approach being pursued would have enabled users to refuse unauthenticated traffic and require it to be returned to sender—with liabilities and costs loaded onto the Internet Service provider who first accepted the traffic and thus had a "contract" with the originator. It would appear that the IETF gave up after a series of bitter clashes over the licensing of patented authentication techniques. The issues and consequences were covered by Andrea Matwyshyn at the Oxford Internet Institute conference on "Safety and Security in a Networked World" in September 2005.[11]

This approach, using technical facilities already built into the routers that currently handle most of the world's Internet traffic, could enable unauthenticated traffic to be filtered and much spam and malware to be traced back to the 200 or so groups said to originate most of it. Others believe it more efficient and effective to make test purchases and follow the payment trail. Either way, miscreants could then be held to account under a mix of criminal and civil law—as most of the main global e-commerce players would wish. Service providers could also contact those whose machines appear to have been affected and "offer" remedial action as a condition of continuing service. That process is, however, onerous and has led to legal and other counter-attacks in the United States. Not all service providers would wish to follow this route and markets might well polarise with some charging extra for filtered services to protected and monitored customers. Another approach currently being promoted is the use of privacy enhancing technologies with identity management systems under user control, enabling users to examine context and site-specific authentication credentials.

If approaches to improving authentication and security are blocked by conflict over the licensing of software and/or business methods patents that is an indictment of those responsible and their use of current IPR regimes. This is, however, a highly contentious area and agreement on any meaningful changes, other than administrative reforms to make the current system work better (eg tests of originality), are unlikely. Instead we should use commercial, political and moral incentives to ensure fair rewards, both recognition and financial, for those who contribute to the thinking and innovation necessary to make the Internet safe for use by ordinary human beings, with the addition of penalties for those who do not, or who actively prevent progress, beginning with public exposure by their peers and moving on to international legal co-operation between those whose customers are at risk.

3.2 *What is the level of public awareness of the threat to computer security and how effective are current initiatives in changing attitudes and raising that awareness?*

See 2.3 above. Awareness is less of a problem than conflicting and impractical advice and guidance. There is a very real risk that further raising awareness without making it very much easier for consumers to protect themselves and their children and to report malpractice will lead to a serious loss of confidence. At the very least the DfES and its agencies should mandate that all publicly funded ICT courses and qualifications include basic computer security and Internet self-protection.

3.3 *What factors may prevent private individuals from following appropriate security practices?*

They lack the training and means to manage their own security effectively, even if they have the necessary awareness and incentive. Most ordinary human beings are baffled by the documentation and "help" routines currently on offer. There is a great deal of advice and guidance currently available but much of this moves rapidly from the simplistic and patronising to that which requires Masters Degrees in Information and Computer Science to locate and understand. And even then the tools that users are expected to install and trust appear to spend much of their time fighting for supremacy within the system—identifying each other as threats to be removed and expecting the user to adjudicate. Some recommended security practices, such as never opening email attachments, seriously degrade the usability of the Internet and are widely ignored. The problem is compounded by commonly used software that silently executes attachments if their internal structure indicates that they are executable without consulting the user.

[11] http://papers.ssrn.com/sol3/papers.cfm?abstract_id=903852

DfES and the relevant agencies (QCA, Sector Skills Councils etc) should ensure that all publicly funded ICT training courses and qualifications include basic security and self-protection. Government departments and their service contractors should, as a matter of course, follow good industry practice and train all users in the secure use of the computer systems to which they have access while ensuring that this is not used as an excuse for undermining good practice on usability and accessibility.

Cabinet Office, Home Office, DTI and DfES and the Police and Law Enforcement Agencies should bring together their various Internet Safety and E-Crime prevention initiatives and link this activity closely with initiatives to open up and promote access.

Internet Service and E-Commerce providers should work with Government and Law Enforcement to ensure their customers have ready access (eg well-promoted portals) to intelligible, realistic and comprehensive sources of advice, guidance and reporting—again, linking consideration of the advantages of technology with the safety issues, rather than leaving it to customers to "join things up".

There is also confusion over the scale and nature of "identity theft", including who is liable for what, when an individual is impersonated. The National Consumer Council has called for an industry-funded service along the lines of the US Identity Theft Assistance Group. However, the latter only handles cases referred by its members. UK organisations like Experian already have dedicated "Victims of Fraud" support teams and provide guidance via Citizens Advice Bureaux and Crime Prevention Officers. There is a view that while existing guidance needs to be regularly updated and better promoted it were better to work through existing channels than create a new one.

Those seeking to promote confidence in on-line transactions should co-operate in producing common, well-promoted portals that provide advice and guidance for those who believe they have been impersonated, as well as guidance on how to reduce the risk and contact details for those who can help remedy the problem.

3.4 *What role do software and hardware design play in reducing the risk posed by security breaches? How much attention is paid to security in the design of new computer-based products?*

We do not need to wait for the re-engineering of the Internet with new generations of routers, browsers, operating systems and addressing systems in order to make serious progress in Internet safety, security and crime prevention. Improving the quality and relevance of the advice and guidance on offer, including to those using existing products to run their own on-line services, could make a massive difference.

One suggested "quick fix" is for the main email browsers to provide default options to disable the automatic execution of email attachments or embedded ActiveX or Java in emails, and also to disable html links inside email. It is claimed that for the vast majority of users the reduction in malware would greatly outweigh the inconvenience.

We need much greater co-operation to identify and promote the best practical advice currently available, in language that ordinary human beings can understand, and to ensure that reputable security products and services recognise each other and co-operate. That process includes giving much greater priority to computer security and Internet safety in mainstream ICT education and training at every level—from schools through further and higher education as well as adult courses on the use of IT, to the design, implementation, operation and support of systems in ways that reduce opportunities for abuse.

It is almost certain that crime-prevention education and practical guidance and support is an area where incentives will be more effective than penalties. The core task is to persuade security suppliers to put a proportion of their current marketing spend and major users to put a proportion of their security budgets into co-operative ventures to promote good practice and competence at every level—including among their public sector customers and partners who are often among the most complacent and vulnerable.

One of the best ways of promoting such co-operation is almost certainly a series of awards for "best of breed", to give the oxygen of publicity to good practice and encourage others to join in or do better. Well publicised awards for:

- products and services with plain language, intelligible and useable documentation, websites and help processes related to what the user experiences (technical merit, innovation and excellence are not enough); and
- producing, promoting and distributing advice and guidance for target audiences (children, parents, teachers, small firms, end-user staff in large organisations etc) in a way that helps the user to understand opportunities and vulnerabilities and to understand the connection between them.

3.5 *Who should be responsible for ensuring effective protection from current and emerging threats?*

The issues are now too serious to be treated as a constraint and left to law enforcement and security experts to do their best with reactive add-ones. There is a need to involve those affected (users and customers as well as suppliers) in well-structured advisory groups to help formulate policy, especially when there are splits within the industry as to what is desirable or practical and who should be responsible.

Safety and security has to be treated as part of the mainstream corporate social responsibility and good citizenship programmes of all those who wish their customers, citizens and taxpayers to make confident use on-line products and services.

In practice that means the active involvement of the major commercial players across the converging communications services (Internet, broadband, mobile and broadcast) plus those running or promoting e-commerce, on-line banking and payment, search engines, distance learning, content and electronic service delivery by government.

Only when major players vote with their wallets, to protect revenues and control costs in the face of changing consumer behaviour (eg a return to branch banking), will the technical, legal and organisational constraints that have prevented effective action to address the problems be overcome, removed or bypassed.

3.6 *What is the standing of UK research in this area?*

Most of the relevant products and services are global. The fact that Hewlett Packard, IBM, Siemens and Microsoft have major security research facilities and partnership programmes in the UK indicates that we still have serious strengths. However, their concerns with regard to the UK science, technology, engineering and mathematics base also indicate that we have serious problems that need to be addressed. Our neglect of multi-disciplinary research into people processes, especially how human beings use systems—including supposedly secure systems—is a major weakness, although this is beginning to be addressed. Indeed it may be one of the reasons why those turning technology into product commonly do so outside the UK.

4. Governance and Regulation

4.1 *How effective are initiatives on IT governance in reducing security threats?*

The European E-Commerce directive requires those trading over the Internet to provide physical contact details in addition to their on-line address. This should provide a significant protection against fraud but many trading sites fail to do so and, furthermore, the registration details obtained by a "who is" enquiry are, if available at all, often those of the service supplier who built or sold the site. The plans of Nominet to amend the contractual conditions under which .uk domain names are registered will help address this problem within the UK but it illustrates the lack of impact of most government initiatives, including EU directives.

The creation of effective frameworks for global co-operation, using the contractual terms of the current registration authorities and of the Internet service suppliers to protect paying customers and remove miscreants, should have a higher priority than the creation of statutory regulatory and governance routines. Unless well judged, the latter not only divert resource from addressing known malfeasance but can create more vulnerabilities than they remove. For example one of the largest insider dealing operations in a western nation was only possible because new regulatory rules had enabled a compliance officer to bring together staff from across the internal security boundaries of the organisations involved.

Meanwhile Sarbanes-Oxley mandates not only expensive paper-chases that would not have prevented Enron but also anonymous whistle-blowing routines of the type made illegal in France after World War 2 because they had cost so many lives at the hands of the Gestapo and Milice. Requirements to give regulatory or law enforcement staff the ability to cross the security barriers of financial services players or to demand the retention of vulnerable data, are obvious examples of how well-intentioned initiatives can cause responsible organisations to move key functions outside the jurisdictions concerned. The cost of ill judged regulation is not just money but can be increased risk, personal as well as financial, if it makes it harder for reputable service providers to provide realistic protection for their customers.

All proposals for new regulatory regimes must be subjected to a full systems review and impact analysis to check how they will achieve the objectives stated and at what cost to legitimate business, given current and prospective technologies and business models.

4.2 *How far do improvements in governance and regulation depend on international co-operation?*

There is much talk of the need for more cross-border co-operation but debates within regional groupings like the European Union over applicable law, including "country of origin" versus "country of destination", indicate that little more progress at the global level is likely over the next decade than has been achieved at the inter-governmental level over the past century. Most of Europe shares common legal traditions but agreement on common frameworks is often hard won. If one then looks wider at the clashes between Roman, Common, Islamic and Asiatic legal traditions, let alone cultural and political differences, including those between the EU and US, the lack of wider progress becomes less surprising. Meanwhile the private sector has had routines for international co-operation for over a thousand years.

The best selling book and subsequent film, *The Da Vinci Code*, were largely inspired by the mythology around the break up of one such network: that which enabled the Knights Templar, the Venetians, the Byzantines and the Arab/Jewish networks of the Middle East to co-operate in transmitting funds safely from the Orkneys to Jerusalem, until the King of France reneged on his debts. Today such routines are not only global but have evolved via routines to handle piracy on the high seas or accidents in space, with adjudication under whichever law and in whichever location the relevant service contract(s) state.

The global financial services, international payment and freight forwarding operations of today have similar routines for handling cross-border transactions between customers operating under very different legal and regulatory systems. Some of these are already integrated into seamless on-line networks, operated from a handful of regional hubs, with local access under the legal and regulatory regime of the nation from which access is being made: country of destination.

The Internet has a different tradition, with regulation largely based on country of origin and remarkably little interference from the government of the nation that, until very recently, originated most of the traffic. Other governments around the world are, however, loath to leave the policing of the Internet to a cartel of global commercial players operating under the governance of ICANN, the Internet Engineering Task Force or W3C, let alone the ITU, IPU or other international bodies. But if that is to be replaced by something better, not mere anarchy, they must greatly increase the resources they provide to their domestic e-crime law enforcement operations and develop very much more efficient routines for cross-border co-operation—using the expertise of the major commercial players in working with and through local law enforcement around the world.

This will not be easy and those in the West who argue that such routines must be democratically accountable should remember that some of Cicero's greatest speeches on republican virtue and civil liberties were in support of the tyrants and organised crime bosses of his day. Inter-government agreement on anything that is effective and meaningful is unlikely other than between states that share political, cultural and legal traditions. Even then it cannot be taken for granted.

The best way forward at a political level is to support the successful work of groups like UNCITRAL (United Nations Commission on International Trade Law) in producing model laws for piecemeal adoption. There is also a good case for attempting to draft a UN Treaty on Technical Assistance to enable smaller states and organisations to make better use of the legal routines already well established for handling international trade disputes. This is unlikely to be agreed but a widely supported draft could be of great value to those seeking models of good practice. We also strongly support the approach agreed at last year's World Summit on Internet Society, where the UK as European President led the way in persuading all concerned that a co-operative approach was needed, rather than "no change" or "international control". There are those who are keen to undermine the partnership approach, and it is important for the Industry and Parliamentarians to work together and with Government to demonstrate the commitment without which a partnership approach will not work—and that would lead to fresh calls for a more rigid and bureaucratic system and/or a breakdown of international co-operation.

4.3 *Is the regulatory framework for Internet services adequate?*

The main flaw with the current regulatory framework is that it does not reward those who seek to protect their paying customers from abuse. Indeed it is said that those who seek to actively protect customers risk losing "innocent carrier" status and incur a liability for being sued when they fail. Those who make no attempt to protect customers are immune from penalty. Meanwhile ill-considered requirements to retain data, whether communications or content, without providing law enforcement with the resource to handle what is already retained, not only impose costs on legitimate business to little or no benefit, but also open up significant areas of avoidable risk. Again, it is essential for industry, government(s) and enforcement agencies to work co-operatively rather than in silos.

We need to remove regulation that already has perverse consequences, not introduce more. In particular, any initiatives that could jeopardise the ability of London to add Internet policing and disputes resolutions to its £30 billion a year international disputes resolution business activities must be subjected to rigorous risk assessment. That is not just because of the potential cost to the UK economy, but because having Internet policing functions based in the UK will greatly improve our ability to protect our own citizens from abuse.

There is a need for industry strength market research into what Internet users actually want and from whom: including by way of trade-offs between price, facilities and security. Additional regulation should be avoided unless there is clear evidence of market failure to provide that which users want and are willing to pay for or unless there is a need to provide regulatory underpinning for "best practice" as developed jointly by the Industry, Government and Regulators.

4.4 *What, if any, are the barriers to developing information security systems and standards and how can they be overcome?*

See 3.1 above. The break-up of the academia-industry, open source and open licence co-operation that created the Internet has led to a mushrooming of add-on, post-event security fixes to ever more complex and competing, commercial and proprietary products and services. Some argue that was an inevitable stage in the growth pains of the information society. Others believe it was but a stage and that customer pressures around the world will drive fundamental structural changes. Meanwhile the current UK and European Data Protection regimes serve to neuter rights of private action and promote tick box compliance. By contrast the US legislation requiring disclosure to subjects of security breaches has transformed awareness and attitudes and given strong economic incentives to developing and deploying privacy enhancing technologies. UK legislation makes it clear that information can be exchanged between public bodies for purposes of crime prevention provided this is done in a professional manner, and this concept needs to be developed further (in both practical and legal terms) in relation to co-operation between Industry, Government and Enforcement Agencies.

5. Crime Prevention

5.1 *How effective is Government crime prevention policy in this area? Are enforcement agencies adequately equipped to tackle these threats?*

The majority of all investigations, including those into traditional physical crime, may now entail securing and analysing potential digital evidence, on the computers, personal organisers or mobile phones of victims and suspects, or from surveillance camera footage that might have covered relevant locations. In 2005, UK business users spent about £3 billion to protect their systems and those of their customers, including nearly £1 billion with security consultancies and suppliers. By contrast the announced spend for all the UK computer crime units, including the child protection and other units now included within the Child Exploitation and On-line Protection unit (CEOP) and the Serious and Organised Crime Authority (SOCA) was £8.5 million. More former policemen with experience of running major computer crime investigations now work for industry than in UK law enforcement agencies.

Those tasked with protecting the most vulnerable and with enforcing the law are playing catch-up, overwhelmed by the scale of criminal and anti-social activity that may require computing or digital evidence skills to investigate. There is confusion as to how (and to whom) on-line incidents should be reported and a reluctance to make it easier to report, lest the result distorts police performance targets, whether or not the latter are in line with public needs and expectations.

Law enforcement lacks the capacity to respond effectively to more than a fraction of currently reported incidents. The Internet has been described as the Wild West without six guns. Law and order was brought to the Wild West by gunmen hired by the railways, banks and citizen's committees to protect themselves, their customers and their communities. A great many agencies claim to regulate content over the Internet but most effective action against malpractice is organised by the major Internet service, e-commerce and on-line banking and payment providers—to combat their common enemies and to protect and re-assure their shared customers. They need to be further encouraged and enabled to act rapidly and decisively, in co-operation with law enforcement agencies, to protect the small firms and consumers whose confident use of on-line transactions and information services is essential to the growth of e-commerce and e-government.

Recent high profile investigations of international paedophile networks show how the resource available to law enforcement can be swamped by the capacity of e-crime to generate very large numbers of incidents and information. The only way of handling the load is through a partnership approach—involving industry staff

and civilian volunteers, working to standards and procedures commonly recognised across public and private sectors, including internationally, as part of joint crime prevention, reporting and investigation operations.

There are many models around the world for such operations: from police "reserves" and "special constables" through accredited security firms and specialist units to industry-funded police forces, such as the British Transport Police. The challenge is to create frameworks that enable local and national operations to co-operate across jurisdictional boundaries, including with nations where the security and probity of law enforcement cannot be taken for granted. This places limits on the ability to use official channels. The routines established by the insurance companies for handling piracy on the high seas and by the financial services and freight forwarding industries for handling international "disputes" are therefore apposite. Managing the interface between formal legal and administrative structures on the one hand and the Industry and informal cultures on the other will certainly prove a real challenge, requiring commitment and engagement on all sides.

Responsibility at the national level for educating, advising and supporting those at most risk crosses departmental and agency boundaries and authority over budgets, courses and curricula is fragmented. At the international level there is much talk but little action, except between those who have met and trust each other, despite the processes they have to use. Meanwhile on-line criminal activity indicates significant co-operation across national and cultural, let alone "family" or "gang", boundaries.

Industry (both users and suppliers) is beginning to co-operate, including with the formation of national and international professional groupings to educate and assess those who can be trusted. The time has come for similar co-operation across law enforcement boundaries (local, regional and national agencies as well as international) with the aim of also greatly improving co-operation with those in the private sector who are working to protect their customers as well as themselves.

5.2 *Is the legislative framework in UK criminal law adequate to meet the challenge of cyber-crime?*

Until this year gaps in the law made the UK one of the safest places in the world from which to run a global e-crime operation, other than one involving child abuse. It was not an offence to defraud a machine, but that loophole appears to have been addressed in the recent update of anti-fraud legislation.

The Computer Misuse Act needed updating with realistic penalties enabling extradition and to address the growing trade in computer tools designed to assist criminal operations. This problem is being addressed in the current Police and Criminal Justice Bill although, at the time of writing, there were still difficulties over wording to enable dual use tools (the computer equivalent of the crowbar/jemmy or picklock) to be supplied to legitimate security consultants while enabling those deliberately supplying criminals to be prosecuted. The Data Protection (Processing of Sensitive Data) Order 2006 now enables credit and debit card providers to receive police data so that they can withdraw cards where their terms and conditions have been broken.

The main residual gap is with regard to realistic penalties for the deliberate abuse of personal information, including those working for the public sector (as staff or contractors) who assist animal rights terrorists, benefits fraudsters, illegal immigrants *et al.* Here, the Department of Constitutional Affairs has launched a consultation to pick up the recent call for action by the Information Commissioner, *What Price Privacy?*

There is a need for early test cases to check that the amendments to UK Fraud Legislation and the Computer Misuse Act have indeed met the objectives. There is also an urgent need to amend UK Data Protection legislation to provide realistic penalties for the deliberate abuse of personal information, as called for by the Information Commissioner.

5.3 *How effectively does the UK participate in international actions on cyber-crime?*

The most important UK contribution to date has probably been to illustrate the value of close co-operation between law enforcement and industry with regard to both domestic and international investigations. The partnership routines being established by the Virtual Global Task Force provide a model for what can and should be achievable. These have greatly improved not only the ability of children to report what is happening to them to someone who will understand and take notice, but also the ability of law enforcement to rapidly track, trace and identify predators. The task force would be very much less effective without the contributions of the industry "partners": from placing the "report abuse" buttons on widely used websites, to providing technology support for reporting systems and investigation, including tracking and tracing communications. Such partnerships need to be imaginative as well as quality controlled. Thus the UK partners include the Football Association as well as Microsoft, AOL, BT and Vodafone.

The result is far more effective education and protection than can be seen in nations that talk about child protection and seek to extend legislation covering television advertising to the Internet, under the guise of regulating video-streaming as a TV like service. It is interesting that some of the latter have rigid divisions which prevent co-operation between law enforcement and industry and recurrent outbreaks of public concern (from press campaigns to mass demonstrations) over the supposed cover-up of widespread child abuse.

This is, however, another contentious area. Some Internet Service Providers, targeting family and business audiences, are happy to introduce robust traffic filtering arrangements and to work closely with law enforcement in identifying predators. Others believe such technologies lead to a false sense of security and are open to abuse, eg covert as well as overt censorship. One of the UK's potential contributions should be to ensure that such issues are debated openly and candidly.

Because child protection is such an emotive subject it also presents excellent opportunities to illustrate how responsible suppliers are already working closely with law enforcement to provide effective education and protection for those at risk and to encourage similar co-operation on a wider front.

Memorandum by the Federation of Small Businesses

The Federation of Small Businesses (FSB) is the UK's leading non-party political lobbying group for UK small businesses existing to promote and protect the interests of all who own and/or manage their own businesses. With over 200,000 members, the FSB is also the largest organisation representing small and medium sized businesses in the UK.

The FSB noted from the House of Lords Science and Technology Committee's press release of 22 March 2007 that the DTI and Home Office Ministers Mrs Hodge and Mr Coaker are giving evidence to the Committee and will be questioned on the costs of cyber-crime to the UK economy and whether the police are adequately funded and have the right skills to deal effectively with cyber-crime. The FSB would like to make its own response to these issues particularly on the point about the costs of cyber-crime to the UK economy.

Costs of Cybercrime to the UK Economy

The FSB "Lifting the Barriers to Growth in UK small businesses report 2006" is based on the survey results of 19,000 businesses in the UK.[12] In the section of the report regarding e-commerce, members were asked about the perceived barriers to e-commerce. The third highest answer, which elicited a response from 20percent of members, cited the risk of online fraud as one of their biggest concerns. This figure clearly shows that businesses are deterred from making greater use of buying and selling online because of the fear and risk of online card fraud, which is dampening down enterprise.

Impact on Small Businesses

The FSB has a particular interest in IT security because the majority of its membership is self employed or runs micro businesses; a third of which operate from home-based premises, without any back up from an IT security department. The FSB's experience is that small businesses are still vulnerable to and fall victim to spam and "phishing" emails from organisations purporting to be major banks or even HM Revenue and Customs, as was a case recently. These sorts of phishing emails are not a new phenomenon but are continually being reinvented and businesses that do not have IT experts or advisers to turn to for assistance are still falling victim. The Government and banks need to do more to educate both the public and businesses to not respond to these types of emails. We do however appreciate the important work and advice available on the "Get Safe Online" website at www.getsafeonline.org.

The Police and Government Response

The FSB calls for better support from both the Government and the police on the issue of online fraud and increased resources put into the police response to tackle it. The FSB welcomes the Government commitment to taking forward the recommendations in the Fraud Review 2006 and hopes that the National Fraud Reporting Centre led by the City of London Police will provide a useful channel for businesses to report, and gain feedback on incidences of online fraud. Wales has recently launched an agency to tackle electronic crime specifically which brings together government, police, academics and business in the fight against online criminals. The agency will track e-crime and make firms better informed about the risks and be more alert to potential attacks. Such an agency does not exist in England and the FSB would support the establishment of

[12] See www.fsb.org.uk

a specific section in the Fraud Reporting Centre which is dedicated to working with business and responding to and giving feedback on instances of e-crime.

Finally, a recent case study of an FSB member illustrates the huge costs that small businesses are forced to pay after falling victim to e-Crime and the lack of police response to follow up on these types of cases. Anecdotal evidence from members tells us that the police do not seem to have any where near the capability necessary to respond to these types of crime effectively. The police need to ensure that the criminals are caught and that the sentencing acts as a real deterrent to other potential offenders.

FSB Case Study

An FSB member runs a concert/night club venue and operates an online ticket office booking service. He was contacted by his service provider informing him that his system "may" have been compromised and was advised to have a forensic audit carried out. The service provider said that this work would cost £30,000 to the business. The member checked that thiswas not a scamand trusted the service provider as he had been dealing with them for some time.

Following discussions with the service provider, the member had a forensic audit carried out at a cost of £9,000 to the business. Independent contacts from the Fraud Advisory Panel said that the business should really have paid around £3,000; however, the business was compelled to use a particular audit company because of requests made by the service provider.

The member has now had to pay a huge amount of money because of the actions of criminals and through no fault of his own. His solicitors tell him that he is actually not covered by insurance in this instance. The member reported the issue to the police but has not as yet received a response.

2 April 2007

Memorandum by Michael Forster (Network Security Architect)

Defining the Problem

What is the nature of the security threat to private individuals? What new threats and trends are emerging and how are they identified?

- Individuals suffering financial fraud (eg phishing, pharming, insecure internet connections, viruses, spyware, insecure email correspondence, insecure web site usage).
- Identity theft with consequential loss (eg insecure public databases with more and more detailed information all in one place).
- Being framed for another's crimes (eg through stolen credit card usage, or abuse of open wireless networks attributable to individuals).
- Some innocents being unfairly arrested on inappropriate evidence (eg some of the victims of Operation Ore).
- Individuals unknowingly breaking the law, or their family breaking the law—both criminal and civil (eg children on music download sites).
- Loss of personal work (eg viruses destroying creative work).
- Loss of reputation (eg people displaying their ignorance by suffering the above).
- Loss of privacy (eg on hacked machines).
- Distress caused to innocent parties (eg children suffering from inappropriate emails, instant messenger abuse, child exploitation).
- IT specialists suffering attention of organized crime and the threat of violence (eg bank security staff held to ransom).
- The loss of availability of IT functionality (eg DOS attacks on DNS infrastructure).

What is the scale of the problem? How are security breaches affecting the individual user detected and recorded?

The cases that reach the newspapers and courts are likely to be a small percentage of all incidents.

How well do users understand the nature of the threat?

Most users see a computer as "white goods", in many ways a computer is more like a car—with similar potential for catastrophe. The misrepresentation of threat levels via press horror stories is also unhelpful, as they can conceal the real facts and issues.

Tackling the Problem

What can and should be done to provide greater computer security to private individuals? What, if any, are the potential concerns and trade-offs?

New PCs being pre-installed with freeware security software with no ongoing subscription requirements eg: Zonealarm firewall (free for personal use) and AVG (free personal edition).

New IT equipment should be distributed with a default of security on instead of off (eg wireless routers with changed admin passwords).

What is the level of public awareness of the threat to computer security and how effective are current initiatives in changing attitudes and raising that awareness?

Generally poor, and somewhere between overconfident and/or paranoid—given the lack of detailed understanding by consumers.

Maybe school initiatives on computer security education issues could help.

What factors may prevent private individuals from following appropriate security practices?

Ignorance of both the risks they are taking and appropriate countermeasures.

The costs of subscribing to the security software as supplied to them by the computer retailers.

The pervasiveness of the computer "White Goods" mentality.

What role do software and hardware design play in reducing the risk posed by security breaches? How much attention is paid to security in the design of new computer-based products?

Generally, more so than ever before by the most successful companies. Clearly Microsoft now see good security as a business enabler rather than a pure cost. There are plenty of companies about, however, that still need to learn this lesson.

Who should be responsible for ensuring effective protection from current and emerging threats?

Clearly, some of the responsibilties lie with:

- Individuals—people can't drive a car without learning to drive and learning the law.
- The IT industry—"manufacturers shouldn't sell cars which are lacking legally required safety equipment and should strive to go beyond minimums." In similar terms, ISPs publish "terms of use", which say things like "you will not spread unsolicited email" (or viruses), and "you will not scan other peoples systems for open ports", but in practice they do not enforce their terms of use unless someone (usually a victim), complains. If the ISPs actively policed their terms and conditions, so that they warned customers as soon as they had detectednon-compliance with their policies, then it would help avoid innocent customers who found their machines being used by malicious 3rd parties, and also warn off any "wannabe" hackers at the first opportunity. In practice ISPs focus on profit and numbers of customers, instead of monitoring their consumer compliance more ethically. ISPs could also do more to offer "secure services" which filtered out aggressive incoming network traffic.

— Business—companies should provide users with as safe an environment as possible to use their equipment to do business with them, and accept some of the fraud risks.
— Government—Police should deter and/or catch dangerous drivers, and the Government is responsible for "highway code", driver licencing, and safety education.

What is the standing of UK research in this area?

The UK security industry is world leading, but this has not been translated into a clear reduction in the risks for UK computer users.

Governance and Regulation

How effective are initiatives on IT governance in reducing security threats?

Some initiatives, eg the NISCC initiatives for corporates, are very helpful. Similar information for the public is less accessible.

How far do improvements in governance and regulation depend on international co-operation?

Significantly, there is no point in local laws in different countries being so mutually exclusive that some companies can no longer legally do business with them.

Is the regulatory framework for Internet services adequate?

ISPs should have more accountability for notifying their users who are (possibly unknowingly) breaking the law.

What, if any, are the barriers to developing information security systems and standards and how can they be overcome?

If there is no public perception of a requirement, and no commercial pressure to provide, then there will not be improvement. If the public want secure systems, and business sees profit in secure systems, (which has started in some areas), improvement can gather momentum.

Crime Prevention

How effective is Government crime prevention policy in this area? Are enforcement agencies adequately equipped to tackle these threats?

While SOCA appears to have enough resource to deal with high profile priority issues, it is questionable if this is enough to support local police forces on less high-profile cases. The lack of qualified forensic experts to support the courts (and reveal innocence where appropriate) is also a potential source of serious miscarriages of justice.

Is the legislative framework in UK criminal law adequate to meet the challenge of cyber-crime?

Potentially it can be adequate, but only if it can react quickly enough to the ongoing rapid changes in potential threats.

How effectively does the UK participate in international actions on cyber-crime?

Clearly more effectively than we have in the past, Operation Ore found many guilty parties, but destroyed the lives of too many innocents.

Memorandum by Prof Steven Furnell and Dr Andy Phippen

SECURITY PERCEPTIONS AND USABILITY ISSUES

Introduction

1. This submission is made on an individual basis and presents material in relation to five of the key questions posed by the Call for Evidence.

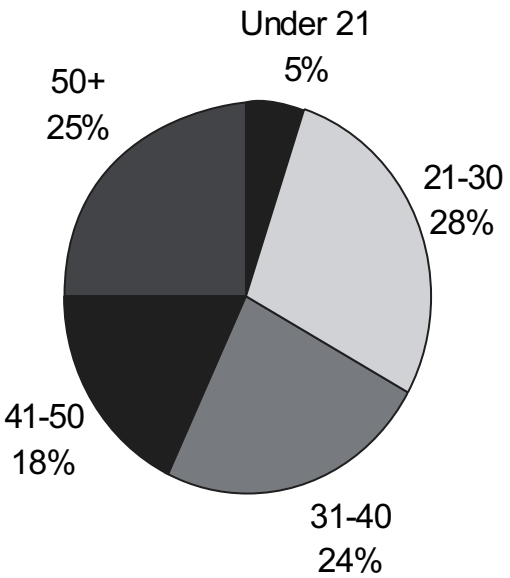
Overview of Evidence Sources

2. The findings presented in this document are drawn from two survey-based investigations (addressing public perceptions of online security and the usability of security technology), and a hands-on user trial which was conducted to supplement the usability findings.

3. The Security Perceptions Survey was mounted from mid-May to mid-August 2006, and promoted to the end-user community via email, word of mouth, and postings to Internet forums likely to be visited by personal users. The survey questionnaire was hosted on a dedicated website (www.securityperceptions.net) and yielded a total of 415 responses (71% male and 29% female), with an age profile as shown Figure 1. All respondents had their own Internet connection (87% of which were broadband), and 92% had been using the Internet for more than three years. The majority of respondents rated themselves as "intermediate" (50%) or "advanced" (43%) level users, with the remainder rating themselves as "novice".

Figure 1

RESPONDENT AGE BREAKDOWN FOR SECURITY PERCEPTIONS SURVEY



4. The Security Usability Survey aimed to assess users' understanding, and hence the potential usability, of security-related interfaces within a number of well-known software packages (specifically Windows XP, Internet Explorer, Word, and Outlook Express). The survey was conducted online during July and August 2005, and promoted via targeted emails and subsequent word-of-mouth, yielding a total of 342 responses with an almost equal split between male and female respondents. The majority of respondents (80.5%) were aged 17–29, suggesting that most were likely to have grown up with information technology as part of their everyday lives. 96.5% of the overall group classed themselves as regular computer users at home and/or at work, with almost 90% rating themselves as "intermediate" or "advanced" users.

5. The associated Security User Trial involved 15 participants in a series of hands-on activities, using security features within a range of software applications. Eight participants were classed as general users, with a familiarity with using IT (and some of the applications concerned) on a regular basis, but with no specific

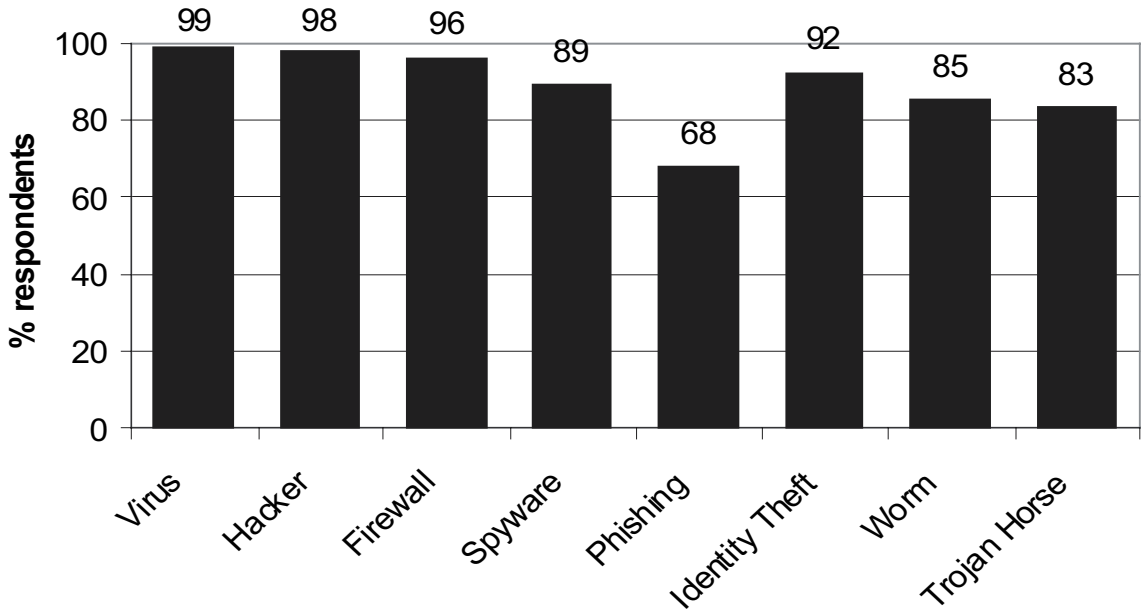
knowledge about the detail of the technology. By contrast the other seven participants were advanced users, all with academic qualifications relating to IT and some prior knowledge in relation to security. The required tasks were presented in writing and explained to the participants. Note that they were told what they needed to achieve, but not how to do it, and the aim of the trial was to determine whether they could understand and use the security features within the application sufficiently well to achieve the objectives. Each trial session lasted between one and two hours, depending upon the ability of the participants and the ease with which they completed the tasks.

How well do users understand the nature of the threat?

6. The security perceptions survey asked respondents to indicate their understanding of a range of security-related terms (mostly relating to the types of threat that they would have been expected to encounter in media coverage). As Figure 2 illustrates, the general findings were positive, but the significantly lower awareness of the term "phishing" is perhaps surprising given the prevalence of the threat at the time of the study.

Figure 2

CLAIMED UNDERSTANDING OF SECURITY-RELATED TERMS



7. A further indication of users' threat awareness was provided by the extent to which they deployed security countermeasures appropriate to personal users, with usage figures of 93% for antivirus, 87% for personal firewalls, 77% for anti-spyware and 60% for anti-spam. However, when asked whether they were aware of the specific role that each of them played, more than a quarter of the respondents were unaware or had only partial understanding. It is also suspected that although they may be using the protection, many users will be relying entirely upon the suitability of the default settings. For example, when asked whether knew how to configure a firewall, or had ever attempted to do so, only 58% responded positively.

8. Although the use of countermeasures meant that the majority of respondents were "satisfied" (51%) or "very confident" (20%) that their computer was secure, a significant proportion remained "slightly worried" (22%) about their system or "not confident at all" (7%). In addition, in spite of their various controls, 46% of respondents agreed or strongly agreed that they felt at risk from online fraud.

What is the level of public awareness of the threat to computer security and how effective are current initiatives in changing attitudes and raising that awareness?

9. The Security Perceptions Survey sought to determine respondents' awareness of a variety of advisory websites that they could turn to for security guidance. Of specific interest were the UK Government sponsored Get Safe Online and ITsafe sites, which were established to assist home users and SMEs, and the findings are presented in Table 1. The overall results clearly suggest that the majority of respondents have not heard of the resources, leading to correspondingly small percentages for those who had visited sites and found them useful.

From a more positive perspective, roughly half of those who had heard of a site had visited it, and similarly half of those who visited one found it useful. Having said this, however, it is also worth noting approximately two thirds of those that had heard of the Get Safe Online site classed themselves as "advanced" users, suggesting that the users most likely to be in need of assistance may be failing to receive the message.

Table 1

PUBLIC AWARENESS OF RELEVANT UK SECURITY ADVICE SITES

	Get Safe Online	*ITsafe*
Aware of the site	11%	11%
Visited the site	7%	6%
Found it useful	4%	3%

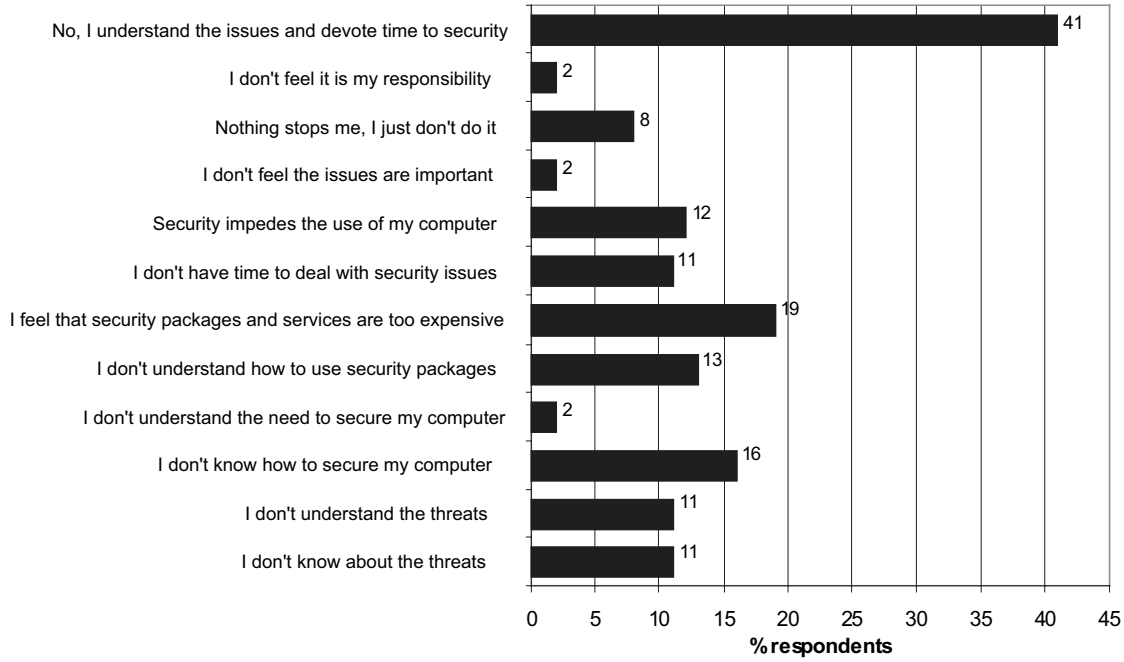
What factors may prevent private individuals from following appropriate security practices?

10. One factor that may have a clear influence here is the extent to which the issue is emphasised when a user buys their system or starts to get it online. Perceptions survey respondents were asked whether they received any security-related information or advice when they purchased their computer or Internet connection. Significantly, 70% responded negatively.

11. Figure 3 illustrates the responses to the question "Is there anything that stops you from carrying out security practices?" While a fair proportion believe that they understand the issues and devote time to addressing their security needs, the remaining respondents indicated a wide variety of impediments. While several of these suggest a requirement for action by parties such as product developers, many also point towards a need for further education of the users themselves.

Figure 3

BARRIERS TO CARRYING OUT SECURITY PRACTICES



12. Other results confirm that the actual level of awareness and understanding is relatively small. For example, questions relating to respondents' knowledge of the existence of security features in web browsers, email clients, office applications and the operating system all revealed awareness of around just 40% (and then

significantly less in terms of respondents' actual understanding of them). Remembering that this was a population in which over 90% rated themselves as "intermediate" or "advanced" users, the findings do not suggest that a more general user population would fair very well.

What role do software and hardware design play in reducing the risk posed by security breaches? How much attention is paid to security in the design of new computer-based products?

13. The comments in this section are drawn from the security usability survey and the associated user trial. Rather than focus upon the full range of software that was evaluated in each context, the results here focus specifically upon the findings from Internet Explorer (which was used by 92% of the survey respondents and already familiar to all of the trial participants). This is considered to be a good candidate for examination, because web browsing is a fairly standard activity for end-users both at home and at work, and represents a context in which a range of security threats may be encountered.

14. The main user-configurable aspects of security within Internet Explorer are accessed via the "Internet Options" within the "Tools" menu. Proceeding from this entry point, the main security options interface is shown, and there are essentially two main elements that a user is required to understand. The first is the concept of different Web content zones, which enable the level of security to be specified differently in relation to the Internet, the local intranet, and for sites that the user has specifically elected to regard as "trusted" or "restricted". The survey asked respondents whether they understood the distinction between trusted and restricted sites, which revealed that 14% did not and 22% were unsure. For each zone, the desired security level is selected via a 4-position slider (low, medium-low, medium or high). Although this may seem straightforward, the challenge comes in understanding what the different levels actually mean. For example, if the user wishes to understand the implications of "medium" security, then he needs to appreciate what an accompanying description such as "Unsigned ActiveX controls will not be downloaded" actually means. In this particular case, the survey revealed that only 65% had even heard of ActiveX, and only 54% of those that had heard of it actually understood what it meant.

15. If users cannot understand the descriptions, then the keywords such as "medium" are their only form of guidance. Thus, although the configuration settings can be used very effectively if users know what they are doing, there is the potential for mistakes. For example, a user who feels particularly concerned about security may be inclined to set the level to "high" for the Internet zone. However, they may then find that legitimate sites no longer work—with the browser sometimes giving no indication that the security settings are to blame.

16. For more advanced users, there is the option to customised the level of protection, and alter settings (of which there may be 30 or so distinct options, depending upon the version of IE in use). However, these options are provided with no accompanying help, and it is therefore likely that very few users will be able to use them (for example, in the survey, only 40% of respondents claimed to understand the subset of options shown in the figure—remembering that this was a respondent group in which many considered themselves to be "advanced" users). A further indication of the poor usability is evidenced when the user leaves the custom settings. Following this, they are only informed that their security is at the "Custom" level, with no indication of whether the actual protection is now lower or higher than the default setting.

Table 2

PRELIMINARY USER TRIAL FINDINGS FOR COMPLETION OF SECURITY TASKS

Task	*General users (%)*	*Advanced users (%)*	*Overall (%)*
Determine the current security settings level within the browser	63	86	73
Determine whether communication with a specific webpage is using a secure connection	13	57	33
Customise security settings in order to permit download of a file	38	86	60
Customise security settings in order to be prompted before running ActiveX	13	71	40
Add websites to the "trusted" and "restricted" Web content zones	86	71	80
Explain the purpose of the Web content zones	86	43	67

17. In the subsequent hands-on trials, the participants were asked to attempt a number of tasks in relation to these elements of browser security. The nature of the tasks, and the ultimate level of success amongst the study group, is shown in Table 2. It is notable that even with the baseline task (determining the current security settings), a quarter of the participants were unable to complete the actions required of them. It should also be noted that even the participants who completed the tasks successfully often took a fairly long time to do so. Such apparent difficulties are particularly notable in an application such as Internet Explorer, which is aimed at the general user community rather than specialists.

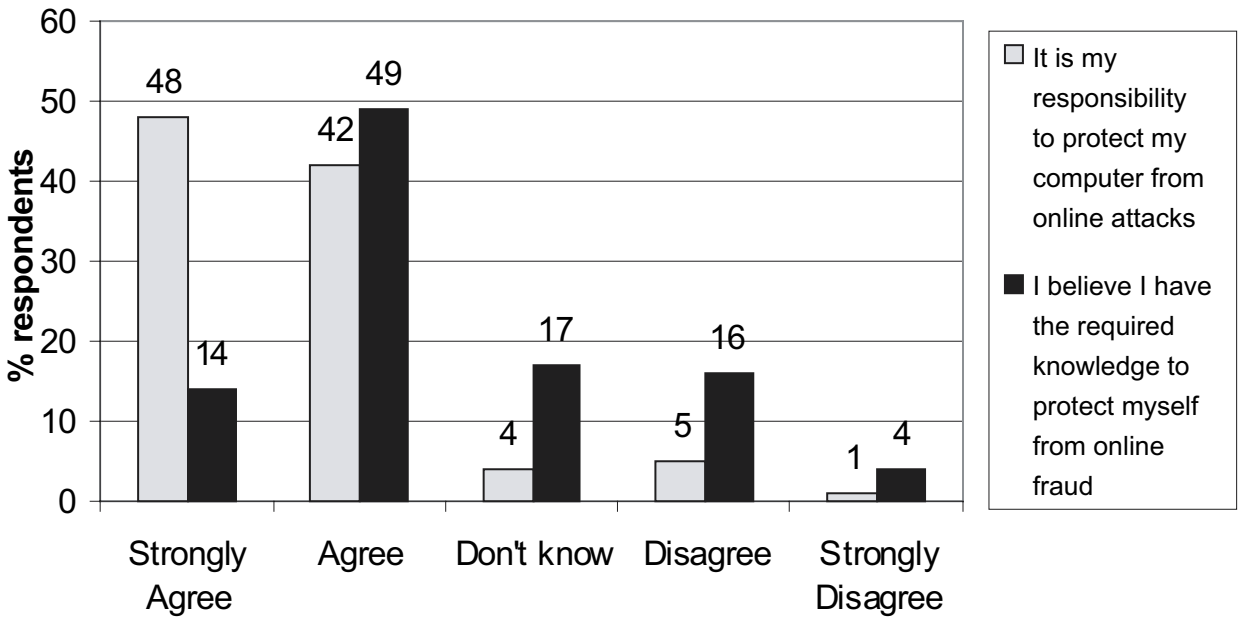
18. Internet Explorer is by no means the only end-user application in which such problems can be identified, and the issue of usability can consequently represent a significant obstacle to effective use of security by personal Internet users.

Who should be responsible for ensuring effective protection from current and emerging threats?

19. Returning to the findings from the perceptions survey, Figure 4 reveals the apparent conflict between users' willingness to take a role in their own protection versus their capability to do so. Although the responses to the statement "It is my responsibility to protect my computer from online attacksine attacks" suggested an overwhelming impression of personal responsibility, a subsequent question in relation to the threat of online fraud revealed that a substantially smaller proportion of users considered that they had the skills necessary to protect themselves (which also links back to the earlier figure of 46% considering themselves at risk from this threat).

Figure 4

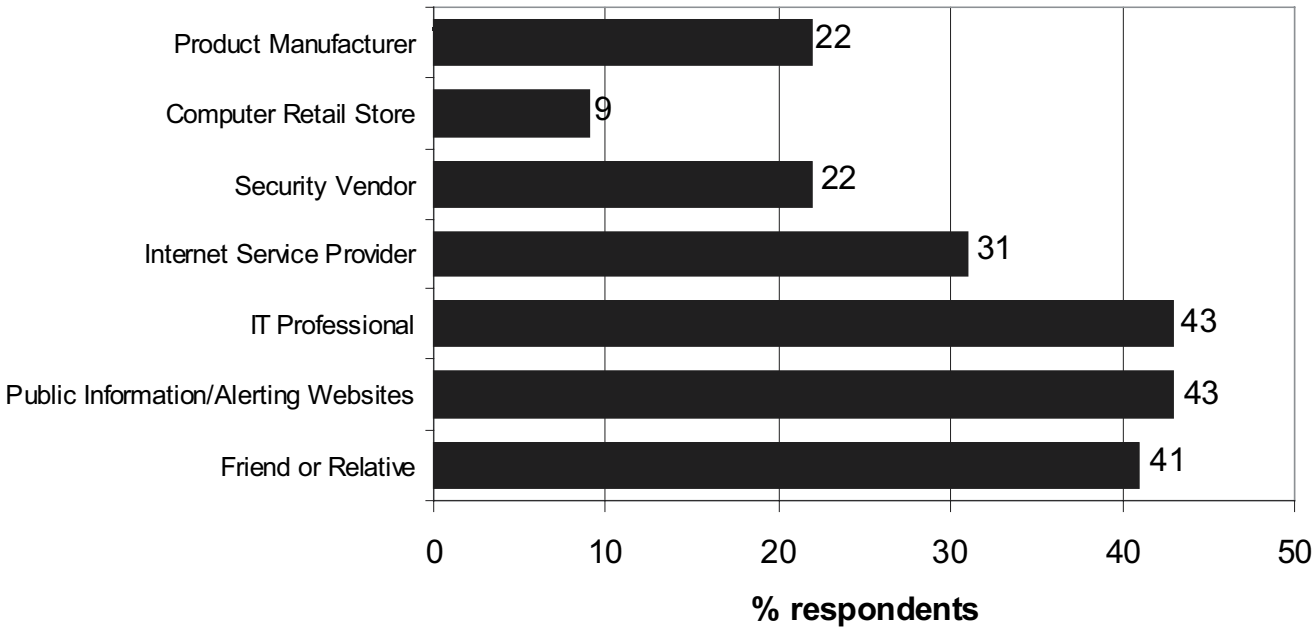
USERS' WILLINGNESS TO ASSUME RESPONSIBILITY FOR PROTECTION VERSUS POSSESSION OF KNOWLEDGE TO DO SO



20. In view of the above, users must still rely upon help and guidance from other sources, and the responses indicate that they have varying expectations about where such sources of advice will be found (Figure 5). It is notable that the "informal"" sources of advice such as friends and relatives score higher than most of the other categories.

Figure 5

SOURCES RELIED UPON FOR COMPUTER SECURITY ADVICE



Acknowledgements

21. The authors would like to acknowledge the significant contributions made by Peter Bryant, Adila Jusoh and Dimitris Katsabas in the conduct of the research studies that have been drawn upon in order to collate this evidence.

17 October 2006

Memorandum by Hewlett Packard

1. HP strongly supports the Government's vision[13] of:

> *"Creating a country at ease in the digital world, where all have the confidence to access the new and innovative services that are emerging, whether delivered by computer, mobile phone, digital television or any other device, and where we can do so in a safe environment".*

2. We would like to direct our comments at helping the Committee understand the nature of the problem and are very willing to provide the Committee with any additional information or help they may need. In particular if members would like to gain a greater understanding of any of the technologies involved we will happily provide experts or host a visit to our research laboratories in Bristol.

Defining the Problem

3. Personal Internet security is, and is going to remain, a moving target. This presents considerable challenges for policy makers in understanding both the nature of the problem and the consequences of actions designed to tackle aspects of the problem. We see four factors contributing to the complexity:

- a rapidly changing technology landscape;
- an increase in organised cybercrime;
- national responses to what is primarily an international problem; and
- poor understanding of individual attitudes to trust, security and privacy.

4. The technology landscape continues to evolve rapidly. The next few years will see a proliferation of devices brought about by communication and computing convergence, new online experiences, richer users of mobility and media, more immersive gaming and greater participation in online communities. Within 10 years

[13] March 2005 Connecting the UK: the Digital Strategy. Cabinet Office, Prime Minister's Strategy Unit, joint report with the Department of Trade and Industry.

we are likely to see significant improvements in display technology, with consequent changes in the way we interact with information. Beyond that, nanotechnology holds the promise of providing ever more processing power at ever less power consumption. It is extremely hard to envision how all this technology will be used, where it will be vulnerable, and where cybercrime will be targeted. In particular, it would seem highly unlikely that security advice five years from now will be based on recommending that you have a firewall and anti-virus software in place.

5. The past year has also seen a rapid increase in organised cybercrime. Newly connected devices are probed within minutes. Consumers remain vulnerable to identity theft and phishing scams, and their machines are often unknowingly subverted to provide "botnets"—the means to launch attacks on more lucrative targets. The security community has little understanding of the epidemiology of virus propagation. And more money can be deployed by criminal groups to find, and exploit, vulnerabilities than it is economically viable for companies to spend on designing and developing more secure hardware, software and services. It is worth noting that many of those who search for exploitable weaknesses are happy to be "paid" in such forms as passwords to porn sites rather than just cash.

6. Whilst recognising that many of the challenges are international, most nation states are focusing their attention domestically. This presents resource challenges for the ICT industry to significantly engage, and also runs the risk of fragmented and inconsistent responses that do little to increase Internet safety.

7. Following the DTI Foresight Cyber Trust and Crime Prevention project's recommendation that more work was needed to understand public attitudes towards trust in the technologies that underpin the Internet and our use of it, BT and HP jointly initiated a study. The project, called Trustguide,[14] was sponsored in part by the DTI Sciencewise programme[15] and completed in October 2006. We would like to draw attention to the findings of the Trustguide project.

Defining the Problem—Trustguide Findings

8. Over a period of 15 months Trustguide ran workshops in the UK with approximately 250 citizens of various backgrounds and ages, who possessed a wide range of interests, levels of technical understanding and personal values. Workshops explored, through the use of current and emerging technologies, where the tensions lie in providing "Internet enabling technologies" that also fulfil personal expectations of trust, privacy and security.

9. The evidence gathered is both revealing and, at times, alarming. Trustguide found that there is a lack of public understanding of the threat or, more precisely, the risks that using the Internet presents. It highlights the considerable challenges of demonstrating to citizens where the systems they use are indeed safe, secure and can be trusted, and where they need to exercise caution.

10. The workshops discussed issues of trust in the context of a wide range of familiar applications, including:

- e-government and public sector IT;
- national identity cards, authentication technologies and identity management;
- data privacy, surveillance and data gathering;
- adequacy of legislative frameworks and education programmes; and
- fraud, theft and the impact on trust in e-commerce.

11. Workshop attendees represented a broad range of citizens, from ICT novices to professionals, children and adults in education, employment and retirement.

12. We believe that the evidence gathered supports the following key findings:

- There exists a high degree of distrust of ICT mediated applications and services (mediated meaning delivered using a range of technologies).
- A majority of attendees believed that it is impossible to guarantee that electronic transactions or electronically held data can be secure from increasingly innovative forms of attack.
- There is evidence that citizens clearly perceived that the threat of cyber crime exists, but understanding is at a superficial level (eg of viruses, spam and firewalls); and felt that they should take actions to protect themselves, but lacked the know-how to act safely.
- Virtually all attendees commonly referred to "risk" rather than "trust" when describing their ICT mediated experiences, and felt more comfortable and secure when restitution existed.

[14] Trustguide website, http://www.trustguide.org.uk
[15] Sciencewise website, http://www.sciencewise.org.uk/

— Lack of control and lack of openness lead to mistrust. Citizens want more responsibility to be taken by government, the banks and Internet Service Providers (ISPs) and for guarantees to be provided.

— Education to enhance personal Internet security is currently patchy and ad hoc across all age groups, most worryingly in secondary schools. Education needs to be accessible to all and at all levels.

13. Trustguide took a "citizen-centric" approach to understanding the beliefs and needs of users in relation to trust, security and privacy in ICT mediated activities and concluded with a set of six guidelines aimed at enhancing the trustworthiness of ICT. The guidelines address the main concerns raised by those who attended our workshops, and cover education, experimentation, restitution, guarantees, control and openness. These and other findings are reported fully in the Trustguide report.[16] An extended summary of the findings and resulting guidelines established by Trustguide, relevant to this investigation, have been submitted separately to the sub-committee through the DTI Sciencewise panel.

14. The study confirmed assumptions that solutions to the problem of personal security are not simply technological and that there is a range of social factors (eg personal risk differences and brand reputation) that must be considered in order to raise the level of trust and acceptance. In particular within HP we recognise the role and importance of corporate brands in engendering trust in individuals.

15. As a technology company we recognise the key role that technology plays in building a secure Internet; however, evidence from Trustguide suggests that technological advancement by itself does little to address the fears and concerns of individuals. Ultimately, it is the way in which we address these concerns that will make those underlying technologies most effective.

Tackling the Problem

16. We believe that greater attention in three areas will help to tackle the problem:

— technology innovation;

— increased professionalism; and

— engagement and education.

Technology

17. It is likely that advances in technology will remove much of the burden placed on individuals today. The combination of virtualisation (providing sandboxed execution and separation of concerns) and trusted computing (providing remote attestation, secure storage and a root of trust) will go a long way to establishing a trusted infrastructure for individuals, businesses and government. In short this is what will make online shopping in a cybercafé safe. Both CSIA and CESG have been highly supportive in encouraging industry to develop and trial these technologies, and UK academics have been keen to work more closely with industry.

18. This summer industry (HP, Infineon, Intel, Microsoft), together with CESG and the German equivalent (BSI), sponsored a European summer school, for graduate students, in trusted infrastructure technologies at Oxford. The formation of the DTI knowledge transfer network and the attention being paid to cybersecurity in Europe with FP7 (the 7th Framework Programme for EU-wide research) all indicate that the UK and Europe has an active and engaged research community.

19. Because HP runs its worldwide security research from Bristol we understand that a key role for ourselves is to couple the UK research base with the predominantly US led IT industry.

20. However the considerable criminal money available to find and exploit vulnerabilities and the availability of social networking and search tools to help mount sophisticated and targeted attacks would suggest that governments would be ill advised to leave technology innovation leadership exclusively to industry.

Professionalism

21. Although cybersecurity remains high on the lists of concerns for CIOs, within many businesses those responsible for cybersecurity feel undervalued and vulnerable. So we welcome the formation of the Institute of Information Security Professionals (IISP) and its focus on increasing professionalism. It should not be underestimated how important the local provision of accredited expertise is in informally helping individuals, SMEs, schools and charities in getting to grips with making their environments safe. It would be extremely helpful if policy makers were able to find ways to recognise and encourage this professionalism, and its deployment for the benefit of society as a whole.

[16] Trustguide publications: Final Report, http://www.trustguide.org.uk/publications.htm

22. NISCC's programme of WARPs (Warning Analysis and Reporting Points) provide an important and successful model for information exchange and increased professionalisation between government and industry. It would be worth exploring whether similar mechanisms could be used to provide information to a larger audience.

Engagement and education

23. The problem has been recognised by many professional and trade bodies and they have initiated activities to engage their members in understanding some of the challenges we face. But by far the weakest link is the lack of continuing public engagement and education. We welcome Get Safe Online and would encourage further measures particularly in schools, not just around existing technologies but in preparing the next generation of early adopters to be smarter in understanding cyber risk and the choices they make.

Governance and Regulation

24. Our engagement with other companies suggests that industry does understand the role it can play in tackling the problem. We have been extremely pleased with the partnership approach to tackling the problem that government departments and agencies are currently taking and believe that this route is the fastest way forward.

25. It is not clear that further legislation or regulation would increase the safety of individuals. And we would strongly encourage much more analysis of the overall ecosystem and who should pay before policy makers consider legislating for restitution. Poorly taken steps, despite good intentions, could easily cripple the UK's ability to take advantage of new technologies and services.

Crime Prevention

26. If cybercrime and cyber enhanced crime continue to increase then it is clear that our enforcement agencies need considerably more support than they are receiving today.

Conclusion

27. HP believes that the UK is doing a lot right in building the community to tackle the problems and we would encourage the committee to look for ways of enhancing and supporting existing activity rather than looking for new initiatives that might spread that community too thinly.

October 2006

Memorandum by Nick Hubbard LLB (hons)

I write in response to the call for evidence on Personal Internet Security.

I acknowledge that I am a security practitioner, engaged in the public sector as an Information Security Officer, and I therefore have a perspective on your subject. But I do not intend to reveal the identity of my employer: this submission is a personal one and not corporate. Unfortunately this denies me the use of my employers' incident records and my comments are therefore largely anecdotal.

I am pleased that Parliament is considering these issues, and I am extremely keen to help as much as I am able.

Defining the Problem

I think it is first worth discussing what the requirement for Personal Internet Security is.

Individuals rarely think through this question, but their requirement is for a system which is readily available for most (say more than 99%) of the time; which does not expose them to significant risk of crime perpetrated against them; and which affords them a reasonable degree of privacy—meaning confidentiality and not being bothered by unwanted material (such as pop-ups, spyware, phishing attacks and spam). The requirement also includes a degree of confidence in the material which is presented to them—so protecting them from fraud, and again from phishing attacks. Like the use of their motor car, they do not expect a perfect standard of safety, but a fairly high one—more so when their families are involved.

There may be a wider issue—that they take it for granted that their personal security is preserved when they give personal information to others on the internet. They do not expect the use of a chat room or a web site to lead to the disclosure to third parties of their information. They expect that organisations to whom they give their information will respect their privacy and related interests (as required by the Data Protection Act 1998 in the UK).

The very idea of a security requirement is problematic in that it is not explicit but assumed and inferred, and taken for granted. That it is only seriously considered after something has gone wrong, when in practice it is usually too late for any satisfactory remedy.

So to the threat. I have heard it said that any offence may now be committed via a computer. The offences of personal harm are more difficult, but one can argue that they are possible. In my five years experience of Infosec, I have seen examples of many of these.

Fraud is extremely common. So are hacking attacks, phishing, viruses and spyware. Hacking on a corporate network is attempted several million times a year. Viruses arrive at the rate of about 20,000 viruses a year. We cannot quantify fraud attempts, but I would guess at around 20,000 attempts per year. We receive more unwanted e-mail than the personal and business-related combined.

At home, my computers are much less active, so attacks are much less numerous. I do not document them, but I regard them as commonplace. About three times a year, I rebuild a machine belonging to friends or family after damage by a virus.

My credit card details have apparently been compromised this summer, for the first time—as a result of an eBay transaction.

More recently I find that my e-mail contains dozens of messages which are from other computers—rejecting e-mails which I have never sent. One obvious explanation for this is a virus on another computer which holds my e-mail address. Another is that my address has been obtained from a web transaction. The first "bounceback" messages were to Thomson@...—this is an address which we have used only once on a holiday company web site (I use this mechanism routinely to trace the source of problems). So it seems probable, but less than certain, that this address was compromised in that transaction: it leaked as a result of accident or otherwise by the holiday company. I feel entitled to expect that they would treat my information with respect: with due care. Now a large number of spam and virus e-mails are being sent—apparently from me. My reputation may be damaged.

So I believe that these events are reasonably commonplace. The threat is very high.

I believe that the threats and trends are the same for home computing as for corporate. But the numbers are far smaller.

Sensitised at work, I apply the same techniques and solutions at home. I spend a huge amount of effort at work on raising user awareness: one of my techniques is to relate the topic to their own information and their home computers.

For many years I relied on the Norton/Symantec solutions. I have come to prefer the BT Yahoo environment, which provides and manages them for me. I recommend that to friends and family. However, since moving away from Norton, I no longer notice attacks on my machines, and I now rely on personal judgement and reports of anomalous behaviour in order to detect breaches. My credit card company, Halifax, and PayPal (relates to eBay) detected the problem with my credit card, much to my surprise, they were very astute.

I believe that a huge majority of users do not even attempt to understand the issue. They follow somebody's recommendations, implement anti-virus and often a firewall, and then forget about security unless/until something goes wrong. So patching and updating virus signatures is largely a matter of luck. They assume that there is a low level of threat, as when they drive their car.

Many users have still only the sketchiest ideas of security problems and solutions because they have very little knowledge/confidence/commitment to their computers in the first place. My parents, my brothers and sister, and my in-laws are a good example of this—of 20 users in my family, only four of us have any interest in managing the computer as distinct from using it. I suspect that is a relatively high proportion.

Many people think of financial details in relation to information security, but my background makes me aware that the interests of my children are inextricably linked with the security of my computer. Their personal information—including habits and venues, descriptions, and possibly sound and images of them could be exposed. The computer can easily be used as a medium to manipulate their actions. Somebody who purports in an e-mail or a chat room to be a 12 year old girl can easily be a 50 year old paedophile.

There is at present very little assurance that any computer-based statement is true or honestly made.

"Spoofing" is easy. I could purchase for a pittance five domain names such as houseofcommons.uk.net for example and thus purport to be a Government Minister—reasonably convincingly and with little chance of detection.

Tackling the Problem

I am deeply impressed by the offerings of BT Yahoo. These allow individuals to implement good levels of security on their computers—firewalls, antivirus, pop up controls, anti-spyware, anti-spam, and parental controls on web surfing, all for a modest price, and requiring a very small input from the users.

Unfortunately, most users are not sensitive to security issues, but are extremely sensitive to price, and competitors are cheaper than BT, so this is making limited inroads into the problem so far.

Many police officers simply reject computer technology as far as they can. Few have any degree of IT competence, let alone in matters of security, investigation of "cyber crime" or the gathering of computer-based evidence.

Cost and effort are critical.

The Government is attempting to lead us towards electronic transactions in preference to the paper and personal ones from the past. These depend upon the availability of a computer—at both ends. To that extent, the private computers are important.

My son and my daughter rely on the Internet for help with their studies. My wife and I use it extensively for all sorts of purposes. The loss would be significant because of their studies; otherwise the loss would be no more than a nuisance. And I believe that we are more dependent on computers than most families. So the availability of the system is not as important as business critical systems (such as the payroll) are within an organisation.

I have a relevant professional position: the personal security of the individual members of the organisation's staff is important. So for five and a half years, I have worked hard to raise their awareness. I cannot quantify the present level of awareness, but I am sure that it is a minority who have taken much notice. An important part of the context is that I am able to provide evidence of incidents which take place—so to prove that security is not merely "just in case". I have never heard our staff refer to national initiatives for security—I believe they are unknown.

I believe that the following of appropriate security practices requires intellect, motivation, effort, and funding. Hard enough for government organisations to adopt, let alone private individuals. In my view, organisations must somehow spoon-feed individuals with sound security.

It is my view that today's PC design traces its history back to a time in which the computers were not linked to networks and could be adequately secured within a locked building. Security has been an addition, made reluctantly.

As most computer products come to market the supplier's priority is to deliver quickly and initiate the revenue stream. As a result, software often matures in patches and modifications made after the product is first sold. And it seems safe to say that security features are rarely a major selling point.

Microsoft XP, for example, has been on sale for several years, with a firewall capability but it is only recently that this capability has been enabled by default.

In the end, only the individual can be responsible for his own security, like locking one's car.

I cannot conceive of successfully making suppliers responsible, especially given the international nature of the business, and the issues of jurisdiction.

It seems to me that in the same way that government influences health issues such as smoking and obesity, there is an obligation to work on personal computer security.

Police forces have a responsibility for investigating computer crime. They have arguably an obligation to prevent crime—including computer crime. But they have very little of the skills and resources to do so. And they are culturally inclined to reject the idea. Chief Constables would presumably say that they have no computer crime problem (because they have no mechanism for addressing it).

The work of the national information security authorities is very important and influential. They provide training and help with the selection of security products, but their target audience is corporate—and primarily in the public sector. And public sector authorities struggle to slowly adopt credible security measures. I believe that little of this work percolates through to individuals' computers.

It seems important to note that the threats and trends of incident change very rapidly. Anti-virus software now needs updating daily to keep up. New vulnerabilities and attacks also emerge daily (see Communications Electronic Security Group publications).

Password technology was perfectly adequate say 10 years ago. But more computing power than ever is available to the mischievous; and password cracking techniques have come on in leaps and bounds. Today a password is fairly unconvincing as a security measure.

It is also important to note that technical defence is only a part of the solution. Some years ago, several individuals in my organisation received a perfectly ordinary uninfected e-mail. It told them that their computer had a virus, and provided detailed instructions. Two individuals followed the instructions diligently and removed critical software components from their operating system. It was a do-it-yourself virus.

Some hoaxes are almost as damaging as the attacks they describe.

Equally "phishing" attacks rely successfully on gullible users supplying information.

Governance and Regulation

IT governance initiatives have some influence in reducing security threats—in corporations, but almost none in the private environment. In my own organisation, we have adopted national standards (in 2001) and we now claim, with honesty, an 83% level of compliance.

I believe that the British Standard (BS7799: ISO 17799) has been extremely useful as a language of security and a model, but only for corporations, and then not for all of them. My Local Authority still aspires to any degree of compliance. Their networks are regularly paralysed by viruses, to the extent of damaging children's education. For example, my son was recently preparing an A Level coursework submission, when his school network failed for about a fortnight. I am aware that teachers routinely carry details of child pupils on laptops which have no effective protection.

Few individuals have even heard of the document.

As the production of hardware and software is international, so governance and regulation must also be international. But it seems unlikely that effective agreements could be reached with enough agility to address the changing problems. So I see this as a fairly hopeless issue.

I do not accept that the regulatory framework for internet services is adequate. But given the jurisdiction and agreement issues, I think that this can never be totally effective.

I am utterly certain that the main barriers relate to awareness and motivation. The Government's drive to e-government was heedless of the security issues. These were assumed to be solvable by practitioners, and to some extent this was true. Government departments are reluctant to adopt sound security practices (the press daily publishes security scandals). Police forces are reluctant and unable to attach any significant priority to their own security or anyone else's, suppliers are motivated by profit—not the interests of the consumers, and there is a very limited public awareness of the issues.

The Bichard Report has gone some way to raise government awareness of the importance of Information Management.

It is my view that Information should now be a Cabinet Level issue—a Ministry of Information is called for if we are to make much progress in relation to the security of corporations or individuals. I believe that Britain plays a leading role in the Information Age—and we should develop it fully rather than stifle it.

I suggest that the police service, and the criminal justice community, should be driven to address computer crime matters competently and adequately.

There is some assumption that computer crime is the work of rather benign nerds. This overlooks paedophiles, fraudsters, mercenary hackers and virus writers. But I do not believe that quantitative evidence is available to define the source of attacks adequately.

Crime Prevention

I am "in the business"; and my enthusiasm is probably evident by now. I am wholly unaware of any government crime prevention policy relating to information.

I do not believe that my local HiTech Crime Unit has the skills or resources to tackle the volume of computer crime. I am aware of the Serious and Organised Crime Agency which may be better equipped to tackle more serious aspects of the problem—I cannot comment on their adequacy.

The legislative framework will always struggle with the international dimension of the problem.

The Data Protection Act 1998 seems to me to be phrased with vagueness—enough to deter most resulting legal action. This act contributes very little to the debate on security and affects only corporations—not individuals. This could usefully be revised.

The Computer Misuse Act 1990 is now well out of date, and is limited to purely technical attacks. It does not, for example, address the issues of the Do-It-Yourself virus I described earlier, and it does not address the issues of Denial of Service attacks.

The Regulation of Investigatory Powers Act creates an offence of intercepting communications, and thus attempts to protect the privacy of e-mails.

It is often said that computers merely provide new avenues for the commission of all the old offences. Older laws such as Theft Acts and Criminal Damage Act create offences which can be carried out through a computer. The legislation was phrased with such clarity that these seem unlikely to cause a problem.

A paedophile may groom his victims through computers, and eventually commit physical assaults. These areas are adequately catered for in the existing criminal law.

Initially there was a great deal of concern about the law of evidence as it relates to computers. But I understand that in practice, there has been little difficulty here. Defendants have not challenged computer based evidence significantly, but we seem to be relying on old principles carried into modern times. I suspect that if and when defence lawyers become IT literate, more difficulties will emerge in this area.

There is one practical problem which remains. It is that it may be easy to prove that whoever used the computer committed an offence: but without an admission by the offender, or some unusual circumstance, it is extremely difficult to prove who used the computers. As I have said, my machines at home are shared by four family members and visitors occasionally have access to them. So in practice, almost anything I do is deniable. The law could specify access controls, or creates strict liability offences, but I do not envisage that either of these approaches would be foolproof.

The problem is not so much the adequacy of the law as the adequacy of the resources required to enforce it.

I am aware that security authorities collaborate on an international basis to prevent, manage and investigate threats. I am aware of very few successful prosecutions resulting from thousands of incidents.

In conclusion, you will see by now that I believe that Personal Information Security is a problem which urgently demands action in several areas: action in relation to suppliers, in relation to awareness of individuals, and in relation to enforcement of the law. Even then some fundamental problems remain because of the international nature of the Internet.

Memorandum by Ilkley Computer Club

Introduction

Ilkley Computer Club is approximately 25 years old. When it started, it was the time of the first micro computers for home use; Ataris, Commodores, Sinclairs and BBCs. Membership was mainly 5th and 6th Formers from local schools. Today, the majority of members are "silver surfers" who almost always use a Windows computer. When the Club started, the Internet had not been invented. Now all members use it and at most meetings, Internet issues dominate discussions.

The members wanted to pool their recent experiences with Internet use and to present them to the Committee in the hope that their collective knowledge—or lack of it—may aid understanding.

Main Points—Problems

- Home users are generally confused by "computer security".
- Clear directed or targeted advice is lacking.
- The inexperienced do not know where to go for advice.
- Most users don't want to spend money on "maintenance".
- Computers are still too complex for most users to understand.
- Users don't know who to complain to if something nasty happens on their computer (eg infestation with viruses).

— There is no understanding of the risks of connecting the home computer to millions of others all over the world.

Main Points—Solutions

— There must be positive Government guidance pushed to users.
— Government advice must be from a single point of contact.
— Internet Service Providers must take a proactive stance in prevention (viruses, trojans, spam, spyware, etc).
— Software produces must take more care when writing software to avoid bugs in the first place.
— Common software for the home user need not be as complex as it is at present (the rush for more "exciting features" tends to produce buggy software of no real use).
— If washing machines can be "kite marked" to EU or UK standards, why not computers?

Government Responsibilities

The overall feeling of members is that there is a lot going on in central government but that the efforts are dissipated around different responsibilities. Often the same general advice is given on several Departmental web sites. There should be one Government "voice" here and one which is well known through a positive marketing campaign through all forms of media.

On a negative note, members considered that the loss of the old National High Tech Crime Unit (NHTCU) web site was a mistake. There was a lot of helpful information on it (eg a check-list on what to do if you thought you had been subjected to ID theft) which has disappeared. This is a good example of not very joined up government.

The Government cannot do everything and must at the end of the day, rely on the home user being sensible and careful. The user must have continuing support from suppliers and manufacturers and this support needs to be presented in non-technical language. The downside is that, for many, there is a reluctance to spend any more on the computer after it is brought home. There is no maintenance schedule for computers. You don't have to take it back to the "computer garage" at regular intervals. There is no annual MOT for computers. For many home (and small business) users, the attitude is to leave it alone.

This is certainly understandable because computers are still geeky things that are difficult to understand let alone tinker with. They are just too complex. Once you always got a thick manual with one but these have disappeared and you need to look up problems on line and this always seems more difficult than flicking through a handbook.

It is also very difficult to know how sensible to be today because today's threats are not quite the same as the ones last week. It is also difficult to for home (and small business users) to evaluate risks, especially when messages are usually full of "doom and gloom". Too many dire warnings are a switch off. An emphasis on positive actions—the best practice approach—may yield better results.

What are the minimum standards of competence needed to own and run a computer? Can this standard be pushed? The ECDL training package says very little about security, for example. How about an official government handbook—short and written simply—which sets out what the home use must do to be safer?

The home use must clearly understand the risks they face when using their computer and have risk minimisation spelled out to them.

Memorandum by the Institute for the Management of Information Systems

The Institute for the Management of Information Systems is the professional organisation for those who are responsible for managing the use of Information Technology to achieve business and social benefit. It has around 12,000 members and is UK-based but the majority of its members now live and work outside the UK; they therefore have an international as well as a practical perspective.

IMIS is an active member of EURIM, the Parliament—Industry Group concerned with the politics of the Information Society and agrees with the points made in their submission. It may, however, be helpful to separately state those points that most affect our members' views on whether the UK is a safe and secure place to go on-line, compared to other parts of the world.

The lack of current UK legal frameworks for effective action against those copying and selling personal data, combined with the collapse of any form of serious immigration control, means that the UK is a "safe haven" for those running much of the world's on-line fraud. Many of the world's phishing attacks may appear to come from Russia or South America but they are said to be often co-ordinated from London and the Home Counties.

— Lack of confidence in the security of the UK Government's own systems is a major obstacle to securing support for joined up information management. ID cards are commonplace around the world but they are "the lead standard": residents' cards for low value or risk transactions. The idea that the UK Government will create a "gold standard" without first sorting out its own notorious information security problems, the start point for much fraud against the private sector, does not command professional credibility.

— Lack of confidence in the security of the systems of on-line retailers is a world-wide obstacle to persuading consumers to use the Internet other than for low value transactions or those where someone else is bearing the risk, as with UK issued credit cards.

Those who wish to halt the erosion of confidence in the UK as a safe place to go on-line, not just in the Internet as a safe place to work, learn and play, therefore face a major challenge, unless they really do face reality and work together.

The key points of leverage appear to be:

Rapid and effective implementation of the recommendations in the Information Commissioner's recent report to Parliament: "What Price Privacy? The unlawful trade in confidential personal information".

The Department of Constitutional Affairs is currently consulting on "Increasing penalties for deliberate and wilful misuse of personal data". There is a need not only for action on this to be a priority in the Queen's Speech but for a high profile test case or two in which the new powers are complemented by use of the existing powers for unlimited fines and action under the Proceeds of Crime Act. We have to demonstrate that the UK is no longer a safe haven for the global trade in stolen and fictional identities.

A major review of the security of Government's own systems, followed by mandatory training in basic information governance and Internet safety for all public sector employees, akin to that done by large commercial organisations, many of whom also make the materials freely available to employees' families.

UK Central Government has often mandated bad practice, under the guise of ease of access, social inclusion, increasing voter turn-out etc. It needs to recognise that all of these are fully compatible with good security practice, provided it accepts the necessity of using trained and supervised human intermediaries to also physically authenticate certain types of transaction. That means understanding and actively managing the risks of unsupervised, on-line activity, regardless of the security technologies used, not just assuming that its supposed cost-cutting potential will always outweigh the problems of fraud and abuse. They may—but very often they do not.

A coming together of those major players, public and private, who wish to see voters, consumers and their families confidently using the Internet to agree common good practice in using existing products and services more securely so that they can also agree on credible advice and guidance for their customers on how to respond to e-mails or access websites.

The major e-commerce and on-line service providers and their business and government customers then need to help organise and fund, the bringing together of awareness programmes like those of "Get Safe Online" and the "Child Exploitation and Online Protection Centre" with reporting routines, like those attached to the Metropolitan Police "Fraud Alert" site and the mandatory inclusion of Internet safety and basic security in all publicly funded ICT education and training.

Only then will the UK be able to realise its potential as not only a safe place to go on-line, but a natural location for global Internet policing, exploiting the unique strengths of the City of London, and therefore the safest place to go on-line.

Memorandum by the Institute of Information Security Professionals

We would like to thank the Committee for conducting this inquiry. The issues raised are very relevant.

We are an organisation set up at the beginning of 2006 and represent Information Security Professionals in the UK and around the world; in addition to over 1,000 individual members, our membership includes leading companies such as Accenture, BT, BP, Camelot, CISCO, HBOS, HSBC, HP, ICI, KPMG, Vodafone, RBS, Unisys, and UBS.

In preparing our submission we have consulted all of our membership and circulated our draft response to the membership for comments. We have also taken input from other organisations such as EURIM and the IET.

About the IISP

The IISP was created in 2006 to represent Information Security Professionals in the UK and around the world. The membership represents a wide range of expertise, from technical experts to leaders in the field, encompassing a wealth of professional experience and knowledge, independent of commercial interests.

The membership in addition to professionals also includes public and private organisations such as Accenture, BT, BP, Camelot, CISCO, HBOS, HSBC, HP, ICI, KPMG, Vodafone, RBS, Unisys, and UBS.

The following evidence has been prepared on behalf of the Institution's Trustees, after inviting input from its membership.

Abstract

It is clear that products and services need to have adequate levels of protection embedded. Moreover appropriate and easy ways for consumers to protect themselves need to be created and shared.

The challenges around Internet security are exacerbated by the rapid evolution of both technology and associated threats. This combined with their general lack of understanding makes consumers a natural target.

The key elements in securing the Internet are to enhance both the level of professionalism in developing secure products and services, and also to recognise those who can provide competent advice to consumer and business alike.

Defining the Problem

The number of computing devices and essential services becoming "Internet enabled" is rapidly increasing, and consumers are keen to take advantage of the convenience and lifestyle benefits of a rich set of services and ubiquitous connectivity.

However the range and sophistication of emerging threats is becoming too complicated for consumers to understand. In recent years we have seen a rapid increase in threats and the situation is likely to worsen.

It is clear that products and services need to have adequate levels of protection embedded. Moreover appropriate and easy ways for consumers to protect themselves need to be created and shared.

Disclosure, and possible abuse, of personal data held on the myriad databases throughout the world remains a threat to consumers and citizens over which they have no real control. They have to assume that organisations to whom they have provided the data in order to take advantage of the services will maintain effective security over this data.

Consumers have for many months now seen a number of companies offering this information for commercial gain. Equally consumers have struggled to understand who to turn to for advice and who is competent to give it.

The key challenges therefore in securing the Internet, are to enhance the level of professionalism in developing secure products and services, and also to recognise those who can provide competent advice to consumers and business alike.

Tackling the Problem

It is likely that some of these threats will disappear in the next few years as new technologies are developed and introduced. We expect an evolving market to develop where consumers are offered more security services embedded into a more resilient intelligent infrastructure. The profession hopes that these changes will make it easier for citizens to take effective measures to protect their own devices.

However to achieve this and for consumers to feel safe in their use of the Internet they will need to have the confidence that those who are designing, implementing and advising on security are competent professionals.

Increasingly products and services as well as advice and guidance are coming from offshore environments, eg Eastern Europe, India and China. It is therefore encouraging that overseas individuals are increasingly approaching the IISP seeking membership.

It is important to promote an environment where products and services are designed by recognised competent professionals and where advice and guidance can come from those same recognised competent professionals. In addition to this education of consumers is essential.

The membership of the IISP has extensive knowledge of the threats and dangers facing the consumer, and although this knowledge is not presently utilised for the benefit of the public at large, many of our membership are enthusiastic about finding ways to help.

Developing partnerships with government efforts such as Get Safe Online where that knowledge is essential to educate people effectively will be of significant benefit to society.

Governance and Regulation

Self regulation is preferred to imposing regulation, and the challenge of regulating in this area is the international dimension of the issues. New vulnerabilities are being identified and exploited, and new ways of combating fraud and other crimes are being performed electronically.

Legislation does need to be maintained to retain a deterrent, however crime prevention/protection is often the best defence. To achieve this, one of the areas that the Government has explored is the issue of licensing information security professionals.

In doing so Government has recognised the importance of public protection and the need to have competent professionals designing and delivering information security.

This need is reflected in the requirement for competent professionals working in the hardware, software and services industry as well as those working in Government, the police, and the education sector.

The Government and large private sector organisations' effort to promote the competency of those working in information security through membership of the IISP is a key step, and one which has been recognised by leading organisations in the public and private sector around the globe.

With this development consumers and citizens alike will have the confidence that those working within the field are able to offer reliable advice and guidance to enable a safer Internet.

20 October 2006

Memorandum by the National Computing Centre Limited

Summary

1. In this response to the House of Lords Science and Technology Committee inquiry into Personal Internet Security, the National Computing Centre recognises that the personal user community is starting to protect itself in certain respects (such as an increased use of antivirus and firewall software) but is exposing itself more through the proliferation of opportunities for self-publicisation (vanity publishing) that the Internet encourages. The energy needed to get to grips with the real and apparent complexities of the measures for secure use of computers is locked in battle with the pervasive complacency that research suggests to be the second to largest, most prevalent risk.

Introduction

2. The National Computing Centre (NCC) is pleased to have the opportunity to deliver the evidence herein on security issues affecting private individuals when using communicating computer-based devices, either connecting directly to the Internet, or employing other forms of inter-connectivity.

3. NCC is the single largest and most diverse corporate membership body in the UK IT sector.

4. NCC champions the effective deployment of IT to maximise the competitiveness of its members' business, and serves the corporate, vendor and government communities.

5. NCC delivers a continuum of services including; independent and impartial advice and support, best practice and standards, personal and professional development, managed service delivery, awareness raising and experience sharing.

6. These services are designed to support IT and IS professionals and their teams throughout their management careers and faciliate operational excellence in the industry. NCC is a social enterprise owned by and run for the benefit of its members.

Defining the Problem

What is the nature of the security threat to private individuals? What new threats and trends are emerging and how are they identified?

7. The security threat manifests itself to individuals in three aspects of privacy risks.
   - The first is the most publicised under the label of identity theft where personal details are harvested with nefarious intent to imitate the victim to defraud them directly, or use the alias to defraud others.
   - There is also a growing trend for vanity publishing of personal details. This may be harmless fun for some but may encourage the attention of "cyberstalkers" or paedophiles to others.
   - Thirdly there is the ease of which information about individuals activities may be posted to the Internet thus making public what may be previously have been expected to remain private.

What is the scale of the problem? How are security breaches affecting the individual user detected and recorded?

8. Research focuses on the institutional experience and so recording is done by, for example, banks who have to deal with the effects of a breach (such as illegally "authorised" transfers of funds). The fear of reputational risk probably adds another level of constraint on the free reporting that would gauge the scale of the problem. It would be difficult to have a meaningful reporting point for individuals who have suffered a security breach as they are likely to expect that the responsibilities for their protection lie with the institution from who they seek recompense. Home users who have certain security countermeasures from some vendors can report breaches which are used to update records. However the key problem to this is the availability of this information and the need to have a particular configuration. There is a wider theatre of victims who will suffer the inconvenience of a security breach—such as a virus infiltration or loss of control during a Distributed Denial of Service attack, and having expended energy in overcoming the problem will not look for any authoritative reporting point.

Note: The last sentence of this paragraph is an example of the communications problem endemic to the whole issue on improving personal security. The majority of the population want computers to access services and are being forced into having to increase their technical appreciation of how they work so that they will understand the need, and therefore means, to defend them.

How well do users understand the nature of the threat?

9. Users do not, on the whole, understand these threats well. They have to:
   - be aware of the threat itself—such as identity theft (we note the coincidence of this consultation with a national campaign to protect against this);
   - understand that the mechanism through which this threat is realised can be:
     (i) technical—such as the covert installation of software to harvest identification details;
     (ii) social—such as e-mails which either play on the psychology of Internet activity like the entering of usernames and passwords into familiar looking websites; and
     (iii) sociotechnical—such as e-mails which goad the user into an action that leads to (i).
   - then understand the solution to the problem which will vary from resisting temptation to open an unexpected e-mail attachment to having to update the software on a computer to prevent many forms of malicious software embedding itself; and

— fight complacency. An NCC survey into the top IS/IT risks identified "Complacency, lack of awareness or understanding of risks, or accepting too much risk" as the second most prevalent potential problem. This reflects the human limitation of misapplying personal experience and discounting past and future risks.[17]

10. Evidence that users would appear not to really understand the problem is shown by the growth in the use of websites which encourage the divulging of personal information (eg myspace). Even if they are not explicitly stating exploitable details, they are passing on the first leads to identity thieves. One might even say that "bloggers are asking for it" by advertising lifestyle and personal details. It has been suggested that the humble "out of office reply" is an invitation to would be thieves to track down unattended property.

11. Examples of this vanity publishing can be seen at:

— http://www.bebo.com/
— http://www.faceparty.com/
— http://www.xanga.com/
— http://www.youtube.com/
— http://en.wikipedia.org/wiki/List_of_social_networking_websites

12. These sites are also an obvious port of call for even more perfidious practices as creating false personas with criminal intent other than identity theft.

Tackling the Problem

What can and should be done to provide greater computer security to private individuals? What, if any, are the potential concerns and trade-offs?

13. There is no silver bullet. An "in depth" approach is needed including:

— Authoritative parenting that prevents—or at the very least discourages—the development of inappropriate web-posting behaviour.
— Continuous improvement of software quality by the developers and service providers to reduce vulnerabilities in the hardware and software.
— More research—and realisation of its results—to enable the distribution of improved software, operating systems and applications, including protective software, to a non-technical audience.
— In-built security tools at levels across the technical spectrum (from network to applications and data) to protect the novice but flexible enough to be switched off by the more expert user who wants to increase their level of protection.

What is the level of public awareness of the threat to computer security and how effective are current initiatives in changing attitudes and raising that awareness?

14. Initiatives are increasing and improving in quality, notably http://www.thinkuknow.co.uk/ and http://www.getsafeonline.org/. However we should ask whether the Internet is the right place to treat the perception and understanding of problems with the Internet? An "in depth" approach using non-Internet-based resources is necessary.

15. The number of helpful sites can be as overwhelming as the incoming phishing e-mail. For example there are:

— http://www.cardwatch.org.uk/
— http://www.codephish.info
— http://www.identitytheft.org.uk/

16. Whist some specialist information can be found:

— http://www.howtowipeyourdrive.com
— http://www.microsoft.com/security/protect
— http://www.millersmiles.co.uk/
— http://www.spamfo.co.uk/

[17] Ian I Mitroff, Harold A Linstone, *The Unbounded Mind: Breaking the Chains of Traditional Business Thinking,* Oxford University Press Inc, USA 1993.

What factors may prevent private individuals from following appropriate security practices?

17. A lack of understanding of the technology leads to a natural lack of understanding of how threats can be realised through that technology. We may expect to see that those attacks which are difficult to detect becoming more costly to deal with as they are likely to have embedded problems into say, several generations of back-up, before being discovered. Personal backing up of data is unlikely to be well practised. Pride in good practice should be encouraged but it must not lead to complacency. Security breaches are like mermaids: just because you haven't seen one doesn't mean that they don't exist. We need to encourage development of trust technologies so that we can let in a few constant friends rather than trying to bar a changing crowd of foes. But don't forget the security in depth principle of not relying on any single approach.

What role do software and hardware design play in reducing the risk posed by security breaches? How much attention is paid to security in the design of new computer-based products?

18. The lesson has been learnt by the software vendors but they are to an extent hostage to fortune that the proliferation of hardware and software means that there is rarely anything new under the sun. New innovation has still to interoperate effectively with legacy technology and the nature of software means that it is almost impossible to guarantee the permutations encoded in a product will secure that product in most (or more) configurations.

19. This is why the in-depth approach combining accountability, technology and education is essential:

- Accountability—Create a system of recognition for legitimate Internet "crawling" software so that Internet Service Providers (ISPs) can block unrecognised (perhaps uncertificated) attempts to harvest information. Legitimate applications (for example, Google, AltaVista, and Autonomy) would bear electronic authenticity certificates.
- Technology—Technology should be developed with mandatory attention to the non-functional requirement of security.
- Education—The responsible use of information technology should be part of the compulsory curriculum of citizenship in schools.

Who should be responsible for ensuring effective protection from current and emerging threats?

20. Now that the Department of Trade and Industry's biannual survey of security breaches in business is making the happy report that the high proportion of businesses are catching the security incidents, it is the time to strengthen the user community with the sharing of the effective measures. It would seem that there is a watershed of attack running from the protected (corporate) to the unprotected (small businesses) and we see this continuing beyond, to the personal users of information technology.

21. Information is passed along a convoluted network of veins, arteries and capilaries, its security is at risk throughout the journey. It is more vulnerable in some places than others. Like the straight Roman roads, we must reduce the kinks and bends where the enemy can lurk.

22. It is undoubtedly good news that more attacks are being detected. We may expect less damage from those which are easy to detect providing defences are strong throughout and we do not get caught by a weakness that is exploited whilst in the shadow of a well defended system.

23. We may never have everyone fighting the information security war. We can recognise that although some may sit and watch, others dive into the thick of it, and some run after with a stretcher, we must always strive for inclusiveness. Where information is managed using technology, understanding all the implications will get technical. Initiatives like "Get Safe On Line" have vital roles but to paraphrase Einstein, it can make the solution as simple as possible but no simpler. Vulnerabilities and patches are "techie". Just as we have seen the Botnets run from the watershed of protection into the trenches of home or small business computing, we need to stem the flow by doing as much as we can to make security measures accessible or automatic. This can be shored up with the increasing desire for professional recognition in information security with a professional institute at its zenith.

What is the standing of UK research in this area?

24. We should be making it easier to achieve commensurate levels of assurance (realising relative security) by paying attentions to lessons learnt from experience. The certification of Japanese organisations to the Information Security Standard BS 7799/ISO 2700 far exceeds that of UK certification. We should consider an investigation of how Japanese individuals may be benefiting by the formalisation of information security management by those who service them.

25. Recent reports have highlighted that (a) Internet misuse has switched from more nuisance to criminal intent and (b) rather than attack defended corporate networks, these criminals are taking advantage of more vulnerable information technology of home and small business.

26. Research is needed into how we may promulgate the lessons learnt by the corporate experience to those who want the benefit of technology without the having to master much if any of its complexity.

Governance and Regulation

How effective are initiatives on IT governance in reducing security threats?

27. It is good that there are initiatives which recognise the "chain" of responsibilities that connects the corporate, public sector, small business and personal information technology users. Only in that wider context can the actions on the individual be put into context.

28. The formalisation of ethics and good governance in the UK, leading to a demand for demonstrable management of operational risk, has largely matured since the last decade of the Twentieth Century. As seems to be usual, the emergent risk of tardily reported inadequacies in high-level governance with the Maxwell pension funds, the Bank of Credit and Commerce International (BCCI), and Polly Peck became the driver. The first set of improvements was proposed by Sir Adrian Cadbury, former chairman of the Cadbury chocolate company, in "The Financial Aspects of Corporate Governance". This was a code of conduct for stock market-listed companies addressing ethical as well as legal questions. The implementation only really became clear when Turnbull prompted attention to risk management.

29. This evolution of benchmarks for corporate governance was given focus by a working party of the Institute of Chartered Accountants in England and Wales (ICAEW). This was led by Nigel Turnbull, so the subsequent documents "Internal Control: Guidance for Directors on the Combined Code" has become known as the "Turnbull Report". Its message is that good corporate governance is achieved by internal controls and risk management. Like Sarbanes-Oxley and Basel II, financial prudence is the driver and a high quality of transparent reporting is a key aspect of compliance. Risks need to be managed and their acceptance must be from the highest level.

30. The ability to put this into practice has been greatly boosted by the Higgs Report which reviewed the roles and effectiveness of non-executive directors in the UK. As a result, the report sets out measures designed to improve the structure and accountability of boardrooms in the UK. This is vital to instil a transparent approach to risk management.

31. Government is concerned with enabling the public and private sectors as well as individuals to achieve secure and resilient information systems. To achieve this, the UK has established the Central Sponsor for Information Assurance (CSIA) to facilitate working in partnership with the public and private sector to address the protection of information systems, the information they carry, and their users from hi-tech crime. The department promotes education and awareness of information security and takes in hand training and skills for professionals.

32. The confidentiality, availability and reliability of information systems and the information they handle is an important concern for Government. The continuous provision of goods and services to citizens depends on the smooth running of the information systems supporting them—particularly in the event of a crisis. But Government cannot make the UK's information systems secure by itself. Most information networks are neither owned nor operated by Government so we each must play a part in protecting all our information systems—from home computers, to the IT networks behind large companies to local and central government systems. In fact we are becoming so interconnected that the contagion from a home computer can spread to business and into Government and vice versa. We need to develop a new culture of cybervigilence which means that we must not only protect our computers from viruses, we must protect our privacy and identity from those who would abuse it. The complexity of the risks requires a scalable approach that can be made to fit the size and place of impact. A risk mitigation framework standards can be designed as to account for the risk and

stakeholder view or weltanschauung in its application. Risks to security are no longer a simple matter of who you keep out; they are a complex and changing set of layers that decide who you let it in and how far. NCC is engaged in the research and development of such a framework.

How far do improvements in governance and regulation depend on international co-operation?

33. International co-operation is important to combat the perception of the relative safety of perpetrators who take advantage of technical and social vulnerabilities from regimes that they feel safe in.

Is the regulatory framework for Internet services adequate?

34. No commentary submitted.

What, if any, are the barriers to developing information security systems and standards and how can they be overcome?

35. Information and knowledge are the thermonuclear competitive weapons of our time.[18] Any information that an organisation holds is an important asset and needs to be treated as such. Risks are inherent in the software driving information systems that store and process that information. It is therefore not surprising that in order to secure information, international consortia (such as the Basel Committee for Banking Supervision) and governments have set out regulations with punitive measures for non-compliance to encourage a proactive response to risk. Individual examples of compliance are knitted together under the banner of good governance so that risks to the disclosure of sensitive, personal information carry national and international obligations rather than allowing the risk of disclosure to be accepted. In addition to the social obligations of the regulatory regimes, information system users are typically at risk from e-crime including the misuse of computer systems for fraud, hacking, virus and denial of service attacks, software piracy, on-line child abuse, extortion and drugs trafficking. In addition to the social protection and e-crime, misuse (deliberate or accidental) of information systems by otherwise legitimate users is still the highest security risk.

36. Regulatory bodies react to emergent risk by creating laws and regulations (social obligations) to promote the environment in which organisations have to manage risk as part of their operations. The drivers for organisations to proactively respond to these emergent, undesirable outcomes are regulatory pressures. According to some recent commentary from the USA this is now less so and the argument to invest in security because of, for example the Sarbanes-Oxley Act, is no longer resonating at board level. Because, although risk management is a continuous process, regulations are seen to be "here and now". In contrast, there is faith that (non regulatory) risks can be avoided. This section discusses how national and international, government, and non-governmental organisations have recognised the need to either establish policies for managing risk or deliver tools to implement policies.

37. National Computing Centre members were consulted on their attitude to standards to investigate whether the hearsay and anecdotes that suggested dissatisfaction in the accessibility of information in standards could be found in a cross section of stakeholders in information systems. The following discussion is collated from feedback collected during this consultation and not previously published. It drew out the opinion that the presentation of standards—and the processes used to develop them—are flawed. It is especially relevant to this paper because it shows how the proposed risk treatment framework can itself mitigate some of these concerns.

38. Standards appear to be unpopular amongst information system stakeholders because of their perceived complexity, the many sources offering apparently helpful standards, difficulties in the visible process of defining standards, the rigidity of compliance requirements, and the cost of the documentation. Each of these concerns is described in more detail below, before discussing how the work to be done in response to the observations made in this paper may help to overcome the apparent consternation towards standards.

39. The complexity of standards is thought to result from the need to try to include not only the intended scope of implementing a technology or process, but also predict the effect of unintentional applications. This results in the perception of much of the information in standards as being preventive and therefore negative. Successful standards are seen to be simple or minimalist, with the emphasis on communication rather than 'prevention'. Although it is undoubtedly important that the impact of proposed changes are understood, it is more important that the need for the change is recognised and accepted by all stakeholders. Leadership and teamwork were cited as the framework for successful projects; standards provide a communications medium within that framework.

[18] Thomas A Stewart, *Intellectual Capital: The New Wealth of Organizations,* DIANE Publishing Co., 1998.

40. The source of standardisation was also noted to be an area of confusion with many contributors to the body of knowledge of IT standardisation. One respondent to the survey cited, as examples, ECMA, ITU, BSI, and ISO. Another respondent referred to the declaration of certain suppliers as being the owners of standards whereas they may have been more successful in penetrating the market place with a particular technology. References by separate respondents to the consultation were made to the remark by Andrew S. Tanenbaum[19]: "The nice thing about standards is that there are so many of them to choose from", referring to the proliferation of standards, and the bawdy "The Matelot's Prayer"[20], intimating a love-hate relationship with standards whose proliferation is not differentiated by quality.

41. The development process in which standards are formulated, reviewed, agreed, and then published was deemed to take too long, have too many roles involved, and be too concerned with synthesising a product that satisfies all view points. The problems were specifically reported as time consuming, bureaucratic and the need to compromise to reach a consensus. The derivation of standards from a series of meetings, will normally take place over a period of years where as market changes and business opportunities seem to be more immediate. The layers of committees and standards bodies mean that it is very difficult to navigate how a standard is progressing or have access to the latest thinking until a consensus is reached. The effort to gain agreement is time consuming and can lead to the omission of useful information that, having been removed during editing, is not circulated to the wider standards audience.

42. Whereas kite marking by the British Standards Institution of certain products such as glass, hot water bottles, and tyres commands a certain degree of respect in the relevant market places, compliance with information system standards—particularly process standards—does not command similar respect where standards are expected to deliver a degree of assurance on the part of the supplier. Compliance is also seen as difficult as there seems to be limited understanding that there is more than just simple pass-fail tests to be applied, particularly in a complex IT system.

43. The cover price of standards is regularly seen as prohibitive, particularly to small businesses who see the full cost in terms of 'cash flow' rather than the benefits that accrue from the implementation of the standard, possibly on many occasions, spreading the cost over more then one project.

44. A framework where standards are linked as solutions to risk may mitigate many of these perceived flaws by making accessible and more obvious, the information in standards that is directly relevant to operational issues. This may be accomplished by using a taxonomy-centric framework that avoids adding any layers of complexity to the standards. A framework may be designed to overcome complexity through navigation based on stakeholder views and "deliver" a standard from one of several sources to treat a risk regardless of bias to the publisher of that standard. The corollary being that the uptake of standards could increase risk awareness and reduce the failures that have given concern over the performance of certificated organisations. Working within the framework proposed in this paper will not make standards cheaper but it could be used to direct users to very specific standards that will offer them value for money through the treatment of otherwise expensive risks. Changes to the bureaucratic standards development process are outside the scope of the commentary in this paper.

Crime Prevention

How effective is Government crime prevention policy in this area? Are enforcement agencies adequately equipped to tackle these threats?

45. Crime prevention policy needs to be embodied in a comprehensive campaign that spans education to encouraging and supporting co-operation between public and private institutions. It should be built on accountability, education and co-operation:

- Accountability—Retailers should expect to only sell "locked down" products which meet the current standard of security "out of the box". Users would be able to accept risk by switching off facilities if they have an appropriate level of understanding to manage those risks. Products could be certificated (for example as an extension of the CSIA Claims Tested (CCT) Mark and retailers could be accredited for their adherence to this approach to security.
- Education—Responsible and acceptable use of information technology needs to be embedded in the education of children and adults. This must range from an understanding of what's safe to do on-line and where different facilities mean different approaches to what they are used for. Transactions from a mobile phone are not the same as transactions from a personal computer at home and are not the same as transactions from a computer in a café or library.

[19] Professor of Computer Science, Department of Computer Science, University of Amsterdam.
[20] 20th Century Royal Navy song.

— Co-operation—Notification of vulnerabilities and breaches needs to be shared so that timely action can be taken.

Is the legislative framework in UK criminal law adequate to meet the challenge of cyber-crime?

46. The UK and the International community needs a framework that encourages disclosure of breaches to ensure that (a) the scale of the problem is clear and (b) the risks that are realised are notified in sufficient time for other potential victims to take preventive action.

How effectively does the UK participate in international actions on cyber-crime?

47. No commentary submitted.

20 October 2007

Memorandum by the National Education Network Technical Strategy Group

Introduction

The National Education Network consists of the broadband networks of the English Regional Broadband Consortia and the regional infrastructures in the Devolved Administrations of Wales, Scotland and Northern Ireland.

The National Education Network (NEN) is also a dedicated education network; it harnesses the power of broadband technology to deliver unique content and services, enabling users to share learning resources. The National Education Network offers many advantages for schools and offers a secure and safe environment where issues such as copyright are managed and where teachers, pupils and parents can work confidently together.

It has recently been noted that the National Education Network, a major government funded ICT project, has been delivered on-time and on-budget.

The NEN Technical Strategy Group comprises representatives from each of the English Regional Broadband Consortia and from the Welsh, Scottish and Northern Ireland devolved administrations with DfES, C2kNI, LT Scotland, Becta and UKERNA. The Group's objective is to advise on the technical strategy required to ensure that such networks interoperate, provide best value and support teaching and learning. The Group also influences suppliers, bearing in mind the substantial government investment in this area.

Although the Call for Evidence refers to private individuals, there is a great overlap between children and young people at home, in the community and at school. While the protection of pupils in school is relatively good through supervision, filtering and education for responsible use, these same pupils become vulnerable outside the school.

Defining the Problem

What is the nature of the security threat to private individuals? What new threats and trends are emerging and how are they identified?

1. The threats include computer virus, trojan and spyware infection.

2. Financial scams and phishing and the consequent loss of confidence in the utility of email systems.

3. The assault on personal values by pornographic and other types of offensive websites and offers of pornographic and offensive material by email.

4. For many, particularly the young, the revealing of private information via social networking sites is a relatively new worry.

5. Young people may also have to contend with bullying by email, instant message or phone (text).

6. We understand that the Internet is being increasingly used by paedophiles to groom children, taking advantage of the difficulty for an individual in identifying who has sent an email or text.

7. In schools we can no longer expect that the material that pupils will see, or that communications with the outside world can be controlled by the school's physical boundaries. An inappropriate email or text message could be received or sent by a pupil in a second whereas only a few years ago a letter or telephone call would have passed through the school office and been noticed.

8. While schools, via their Local Authorities and Regional Broadband Consortia, have the best filtering systems available, the cost of their purchase and management is a drain on limited funds.

9. All teachers are suddenly in the forefront of guarding against a new threat which may make them feel personally unsure and uncomfortable.

What is the scale of the problem? How are security breaches affecting the individual user detected and recorded?

10. The scale is huge, with spam comprising more than 80% of email for many people. Although many are learning to ignore such material, some are deeply affected and may even believe they have contributed by some mistake they may have made in their use of on-line systems.

11. Any Internet connected computer will be infected within minutes by viruses or spyware unless protected. Users may not realise that their computer has been affected until its performance slows to a crawl. Security problems are rarely reported by private individuals.

How well do users understand the nature of the threat?

12. Such threats put perfectly honest people into indirect contact with con-men and thieves without a conscience, this situation may be difficult to cope with. While many users understand in general terms about spam, viruses and scams, some users continue to open email attachments from unknown senders.

13. Few users will have access to real expertise in making a computer secure, unless they purchase their computer with security software installed and enabled.

14. Young people's understanding of the nature of security and safety threats varies with age. More mature pupils will have probably developed some on-line safety strategies—better than their parents in many cases. However most young people probably underestimate the threat, for instance the considerable lengths that an adult might go to groom a young person. Some young people engage in on-line or phone bullying.

15. It is probably also true that—out of school—the wide availability of pornography on-line has degraded young peoples' expectations of relationships.

16. Some parents understand the nature of the threat and take appropriate action to work with their children to minimise risk. Most parents, however, do not understand the threat and are therefore incapable of managing the risks taken by their children.

17. Teachers have embraced the Internet to a large degree although they have far less time available to develop their skills as compared with their pupils. Many teachers will have purchased their own computers and home Internet access, at least partly to prepare themselves for their professional work. In terms of using on-line systems in their teaching the security and safety risks are mostly mitigated by precautions taken by the school networks.

18. Many teachers use of the Internet is probably less exploratory and less wide-ranging than that of pupils. Teachers will need to develop a better understanding of the risks involved in order to better advise their pupils.

Tackling the Problem

What can and should be done to provide greater computer security to private individuals? What, if any, are the potential concerns and trade-offs?

19. We note that these threats are caused by unsavoury people rather than by the technology itself, and that the technology brings a wide range of benefits to education that Internet use is now a normal and essential part of learning.

20. Young people are to some degree used to risk and generally learn how to survive in a dangerous world. Engaging with young people to help them develop their innate ability to detect threats and to respond appropriately has to be the most powerful approach.

21. Clearly we have also to use technological counter-measures such as anti-virus and filtering, but these measures will never completely eradicate undesirable material. Supervision and education are just as important.

22. More work is required by all filtering system developers to produce products that directly relate to the UK schools market rather than a world-wide commercial market.

23. The Becta work in approving Internet Service Providers for safety and security is to be applauded but needs to engage more deeply with a complex problem.

24. For some time schools have used filtering systems to prevent access to undesirable materials and intercept and monitor inappropriate messages. Senior management must take greater responsibility for managing these systems to ensure that decisions are based on educational policy, rather than technical convenience.

25. The biggest issue is in homes where many young people have open access to the Internet if they wish and parents may have little control. There is plenty of material available to help parents, but it is believed that many do not actively respond to the threat.

26. The business case for the perpetrators of much of the more annoying spam is based on a small minority of people responding to what virtually always turns out to be a con. It would be good to think that if people were better educated never to respond, the business would collapse. An essential strategy is user education.

27. It is good to report the recent increase in appreciation of the problems in some schools through the work of CEOP and Becta. However to engage with all pupils in all schools is a massive task that requires well trained staff to be effective. The current level of resource available is far too low to enable excellent programmes such as Think U Know to be widely disseminated.

28. The computer operating system must be as secure as possible and arrive installed on the computer with all the tools required and configured ready to work out of the box. An issue here is that incorporating all security in the operating system may increase the Microsoft near monopoly and stifle competition. Ideally Microsoft would work in partnership with many specialist security companies.

29. The industry must be encouraged to offer secure systems with a minimum of complexity and requirement for user expertise. The splitting of the countermeasures into antivirus, anti-spam, adware, spyware etc may be good for business, but can confuse the customer. IT systems must be fit for purpose, which includes security.

30. A major issue is that many communication systems enable the sender of a message to hide their identity. This may be as simple as mike5476@yahoo.com, but is Mike aged 13 or 30? Where does he (or she?) live? We do not want to enter the debate on national identity cards, but if at least school-age pupils could be certain of the identity of other school-age people then security would be improved.

31. The work by Becta, UKERNA, the Regional Broadband Consortia and others on authentication including the Shibboleth system is therefore important.

What is the level of public awareness of the threat to computer security and how effective are current initiatives in changing attitudes and raising that awareness?

32. Public awareness is probably high, but only to the extent of being aware of email spam, pornographic material and viruses. Awareness of their responsibility in reducing the threat is far lower, for instance most parent worry about their children's Internet access but relatively few ensure safe systems or even check what their child is accessing.

33. Becta has recently produced excellent publications on e-safety which deserve wider reading in schools. The Local Authority is best placed to offer advice to schools on e-safety and child protection although resources are stretched.

What factors may prevent private individuals from following appropriate security practices?

34. Lack of knowledge about basic computer configuration and security, which is not surprising as few in the population are technical.

35. Bad experiences with security software that does not install easily or does not appear to work fully.

What role do software and hardware design play in reducing the risk posed by security breaches? How much attention is paid to security in the design of new computer-based products?

36. It is essential that new products are very well designed. Many security threats make use of flaws and vulnerabilities in the systems attacked, particularly in operating systems where the predominant system is Microsoft Windows. More work is required from Microsoft to ensure it offers the most robust operating system possible, without locking down the computer such that it becomes difficult to use.

Who should be responsible for ensuring effective protection from current and emerging threats?

37. It would be a mistake to attempt to ban Internet applications such as social networking sites (Bebo etc). It is often not the site itself that is the problem, for instance Bebo provides a free and easily-used application for mature people to publish material and to connect with like-minded people. The problem is in users that are too young or naive to see the dangers in publishing personal information or in trusting someone whose identity cannot be verified. Of course some social networking sites make their money through dubious advertisements for finance.

38. Social networking sites, however, must bear the responsibility for ensuring that the young user cannot access the site. It is appreciated that currently there does not seem to be a mechanism to make this possible.

39. Schools bear the responsibility for the safety and security of their pupils whilst on site or on school business. This is not a trivial task and the training of staff with this responsibility is important and currently sometimes neglected. Responsibility for e-safety covers pastoral, technical and educational aspects and all these staff will need to develop their abilities and procedures particularly in working together to resolve these complex issues.

40. Schools also have a responsibility to educate pupils for safety, even if the risk is more out of school than in. We appreciate that adding material into the curriculum is a further strain on teachers and time, but this is now essential.

What is the standing of UK research in this area?

41. This difficult for us to judge. However we believe that UK work is well thought of in other countries. It should be said that some countries feel that in the UK we veer to far towards regulation rather than educating young people for the responsible use of the Internet and related technologies.

Governance and Regulation

How effective are initiatives on IT governance in reducing security threats?

42. UK-based firms are now taking a more responsible attitude to security and this is presumably at least partly due to better IT governance. However the vast majority of Internet security threats would appear to come from America and many other parts of the world where regulation is poor.

43. At UK government, Becta and Regional Broadband Consortia levels there is a good focus on governance in e-safety policy for education.

44. However at school level there is some concern. Many schools have not considered sufficiently at senior management level, the need to create and maintain an e-safety policy and in particular the need to ensure its implementation.

How far do improvements in governance and regulation depend on international co-operation?

45. The Internet itself is international, which is one of its major contributions and benefits but also a source of difficulty in regulation. Many of the IT suppliers of network equipment, operating systems and security and filtering applications are international and depend on that larger market for income to cover their research and development work, partly in countering criminal exploitation of the Internet.

Is the regulatory framework for Internet services adequate?

46. We are not qualified to judge. However with the rapid rate of technology development and exploitation by the criminal and the slower development of user knowledge it would seem unlikely that regulatory frameworks are adequate. However care must be taken to ensure that reputable firms which contribute to developing safe and secure systems are not restricted by over-regulation while parasitic organisations and those that give insufficient priority to protecting users' safety and security are brought into line or penalised.

47. It is essential that schools protect their staff and students by obtaining Internet services through a high-quality educational Internet Service Provider (ISP). Typically the ISP will be carefully selected by the Local Authority or Regional Broadband Consortium. Becta is developing an approvals mechanism for educational ISPs.

48. It would be easy to inhibit Internet use in schools by insisting on a "one size fits all" regulatory regime based on eliminating all risk. Schools must be able to decide how to educate their pupils to take a responsible approach to many risks including drugs, bullying and road safety as well as Internet use. Schools need to set their own policy for e-safety, some will emphasise regulation and some emphasise education depending on their pupils' age and maturity.

49. One of the difficulties is that a school can opt-out of the Internet provision that the Local Authority or Regional Broadband Consortium offers. While this is a small minority of schools, these pupils are being placed at risk as non-educational Internet providers rarely have adequate filtering, security or user-support in place. Indeed as their prices are lower, it is economically impossible to offer these services.

50. There is a danger that if the central funding provided by Government for school broadband Internet access is reduced, some primary schools may decide that they cannot afford the high-quality and secure LA/RBC solution.

What, if any, are the barriers to developing information security systems and standards and how can they be overcome?

51. Becta is undertaking excellent work in moving UK schools towards a standards-based approach to the design of IT systems. Standards for hardware, software, networking and safety and security are an integral part of this development. RBCs have contributed to this work.

52. The barrier to the adoption of standards is often at school level where technical staff have their own local interpretation of network design and may be resistant to change. School senior managers often do not have the expertise to challenge their technical staff, which are anyway difficult to appoint or retain.

53. Due to the increasing devolution of funding to schools, few local authorities have sufficient technical strategy staff to influence schools, which in any case are to a large extent autonomous in their decisions as to ICT.

54. If broadband grant funding were to be completely devolved to schools in the future, such influence that RBCs and LAs have in educating and influencing schools towards standards-based systems and in implementing safe and secure IT systems would be very much diminished.

Crime Prevention

How effective is Government crime prevention policy in this area? Are enforcement agencies adequately equipped to tackle these threats?

55. It is good to report that local police forces are beginning to work with child protection officers and education departments to counter threats to school pupils and to children outside school. Some schools are in the process of giving responsibility for e-safety to a member of staff.

Is the legislative framework in UK criminal law adequate to meet the challenge of cyber-crime?

56. We are not qualified to comment on this, except to say that new threats appear frequently and at huge scale, as seen in social networking. The legislative framework must move at least as fast as the problem, or at least the ability of the interpretation of law.

How effectively does the UK participate in international actions on cyber-crime?

57. Again this is difficult to comment on. However the vast majority of illegal material is generated abroad and the international dimension is vital to its reduction.

October 2006

Memorandum by Paul O'Nolan

The following is submitted in a personal capacity. I have 20+ years experience as the head of IT depts of biological research institutes. Currently I manage a network of over 1,000 computers with a few dozen servers, several Internet connections and one advanced research network link. At the moment I am leader of a World Bank funded project to improve the IT security and business continuity of 15 international agricultural research institutes of the CGIAR.[21]

[21] www.cgiar.org

Much of what I could tell you I am sure you will discover anyway from other submissions (eg 95% of the world's email traffic is now spam coming from "zombie" computers) so I will focus mainly on one issue that may not otherwise get a hearing, what I will call the forgotten victims—those in the developing world. However, I recommend the cover story on 17 July 2006 issue of *Business Week* (The Plot to Hijack Your Computer) as essential and very accessible reading, though trust that this will have been drawn to your attention already.

In the developed world much of the focus on Internet security is on identity theft and financial loss that may result. Notwithstanding the fact that the notorious ILOVEYOU virus originated in the Philippines, that so-called 419 scammers hail mostly from Nigeria and that a growing share of the world's spam originates in China, it is nevertheless true that people in developing countries connecting to the Internet today are the least able to address the consequences of IT insecurity, both in terms of paying for technical solutions where they may help and in having the knowhow to manage them.

I have seen children in the developing world receive pornography by email as their reward for having an email address. I have read that the business of putting children in front of webcams and abusing them is a booming business in the Philippines, a sad but perhaps unsurprising result of the coincidence of poverty and technology.

I ask only that some consideration be given to these issues, which are not simply technical matters but are at some level matters of national morality. There cannot fail to be negative repercussions for societies that tolerate the abuse of the dignity of others and most especially of children. Civilized countries hold child sex abuse overseas to be a crime. Any activities involving technology that corrupts children directly, or sexualises them prematurely by ramming advertisements for pornography, viagra and sex aids etc. down their throats should, in my view, also be a serious criminal offence and all children, worldwide, should be equally entitled to whatever legal protection is available.

There are no technical solutions that would enable spammers to avoid emailing pornography to children but if that were an offence with serious sanctions I believe that this would help protect children and, as a side effect many would welcome, dramatically reduce the incidence of this kind of email.

I believe that the appropriate yardstick for measuring sanctions for inflicting IT insecurity should be the impact on the most vulnerable. If a farmer in a developing country can show that an IT security problem inflicted on him has cost him a proportion of his income then that would be an appropriate cost to the perpetrator. Just as fake drugs have cost lives in the developing world I think it's likely that IT insecurity has also, eg in hospitals.

I have been involved in connecting agricultural scientists in the developing world to improved communications for almost 20 years. I have been involved in the donation of hundreds of computers to schools in the Philippines every year for seven years. Happily most are not Internet connected—yet. Some of what the developing world is exposed to, forcibly, as it comes online churns my stomach.

The United States has failed utterly to introduce workable legislation that would have an impact on the problems of IT insecurity originating in the US. Good legislation in the UK can have an impact far beyond the UK. Global norms will be necessary. The UK can lead the way. I commend the Committe for its interest.

Speaking from the perspective only of an IT manager:

The general public will never be technically adept and operating systems will never be secure. The public will, unavoidably, have to learn more, just as drivers must pass driving tests. However, what people can get away with in small print of software licence agreements will remain an issue. Today every computer user is accustomed to clicking "I Accept" routinely, just to be able to work. It's incontestable that nobody has time to read the small print of every agreement they must consent to in order to install software. Many of these are very bad agreements which should conflict with statutory rights. Imagine for a moment if people were offered 20 page legal agreements to sign every time they got on a bus and if their homes were burgled as result of something they'd signed; or which someone else using a borrowed Oyster card may have agreed to, without any signature. This would rightly be seen as intolerable and would be stoppped at once.

I would welcome seeing Americans—and nationals of other countries with reciprocal agreements—extradited to the UK to stand trial for violating UK laws about deceptive software licence agreements that caused people's privacy to be violated, their identities to be stolen, their computers sabotaged, their bank accounts plundered, their bandwidth wasted etc.

Finally, I can attest that the cost of fighting viruses, spyware, and spam as well as hackers and denial of service attacks is large and is a growing part of my job. It is a tax that nobody should have to pay. Any reduction will free resources for more productive use. In the case of my employer that is spending money, including British taxpayer's money, on fighting poverty, hunger and environmental degradation.

Memorandum by Orange UK

1. Introduction

1.1 The Internet is changing our lives. However, if we are to maximise the opportunities it offers we have to be confident that we can use it securely and as free from abuse as possible. To this extent Orange welcomes the House of Lords Science & Technology Committee inquiry into Personal Internet Security.

1.2 This is a timely inquiry. Not only are more and more people using the Internet to go about their everyday lives but it is now mobile. Orange offers both fixed and mobile Internet services in the UK. We are no longer just a mobile communications business. In June 2006, we integrated with our sister company, Wanadoo, one of the largest Internet Service Providers (ISPs) in the UK, and under one brand—Orange—we are now able to offer consumers a "one stop shop" for all their communications needs: at work, in the home and whilst on the move. These include broadband, fixed telephony (including voice calls over the Internet), interactive "on demand" TV (coming soon) as well as the mobile communications we already provide to over 15 million people in the UK.

1.3 Access to the Internet has become an invaluable communication tool for almost everyone, whether in business, at school or college, in the home or on the move. For work, learning or entertainment it is changing the way we do things—such as buying goods or services, banking, seeking information, listening to the radio, watching television or chatting and interacting with friends—and challenging our traditional cultures, such as enabling more flexible work patterns and transforming consumers into producers (via social-networking user-generated content sites such as Bebo, MySpace and YouTube). A world without the Internet is unthinkable, particularly for young people who have grown up with it. It is also transforming the lives of the older generation or those with disabilities by giving them access to online services (for example banking or shopping) when mobility may be restrictive.

1.4 Demand for broadband connectivity continues to grow offering richer and higher-bandwidth services, such as interactive entertainment and communication. 72.6% of UK Internet connections are now broadband.[22] However, this figure does not include mobile Internet figures. Accessing the Internet whilst on the move is available via high-speed Third Generation (3G) mobile networks, allowing people to retrieve services when on the move rather than at a fixed place, such as a desk or in the home. The pace of change means higher speeds—both fixed and mobile—are ever increasing, making a greater range of services available.

2. Enhancing Personal Internet Security at Orange

2.1 Personal Internet security is a high priority at Orange. The challenge for a fixed and mobile Internet Service Provider is to put in place stringent security requirements without compromising the benefits of the Internet and the development of innovative services. We believe a self-regulatory approach will best achieve this.

2.2 Our strategy is therefore designed to help cut-out illegal or unlawful activity (including spam, "phishing" activity and illegal content) and restrict inappropriate material (such as gambling sites and adult content) to those over the age of 18 years. We work very closely with the Home Office and the Child Exploitation and Online Protection Centre (CEOP). Orange is a member of the Home Office Taskforce on the Protection of Children on the Internet and the Internet Watch Foundation (IWF) and we work closely with children's charities and law enforcement agencies.

Fixed Internet

2.3 Orange is at the forefront of the local loop unbundling revolution. All our current products (broadband and pay-as-you-go (dial-up) come with:

- a free privacy service with parental controls to protect customers from offensive content and to keep personal information safe from hackers;
- a 20% discount on an Internet security package;
- a free 30 day trial of anti-virus software; and
- anti-spam and anti-virus filters for webmail.

2.4 We are working towards implementing a solution which will prevent inadvertent access to illegal child abuse images whether they originated in the UK or from abroad for all our customers before the end of 2007.

[22] Office of National Statistics: June 2006.

2.5 Orange has a dedicated team who deal with all abuse reports (fixed and mobile) and who work to ensure that "spam" is managed effectively. We also work very closely with industry on reports of "phishing" that are prioritised and resolved as per agreed processes.

2.6 Orange aims to make its chat rooms as safe as possible for users. The age for entry into our "teen" chat rooms is 16–19. We do not allow person to person (sometimes referred to as "p2p") chats in "teen" chat rooms and we have moderators on duty patrolling the service at all times. We employ professional moderators, who each undergo a Criminal Record Bureau (CRB) check, in order to protect our chat room users. Moderators are appointed to oversee our services in order to facilitate a cleaner and safer environment. Moderators can ban users or remove anyone from the service who doesn't adhere to our terms of use. Our chat service has compulsory registration with email verification and a clearly marked "report abuse" link.

2.7 The page leading to our adult chat rooms contains an Internet Content Rating Association (ICRA) "tag" allowing parents or carers to use parental controls to prevent children from accessing the adult chat rooms.

2.8 Orange is working closely with the Home Office to produce guidelines for the safe use of social networking sites.

Mobile Internet

2.8 The Internet is now mobile and its availability over mobile networks, including high speed 3G networks, is growing. This can be done using a mobile handset or connecting a mobile "datacard" to a laptop. 12.3 million people accessed the Internet using a mobile network in the UK during June 2006.[23]

2.9 Being able to access the Internet at a time and place convenient to the user opens up a whole new range of benefits, including location-specific information such as traffic news and information. However, the very nature of mobile communications means that services such as the Internet are no longer tied to a fixed place such as the living room. The monitoring of a child's use of the Internet is therefore not as easy.

2.10 Along with the other mobile network operators, Orange recognised the potential dangers of making the Internet mobile. In 2004 operators published a Code of Practice for the self-regulation of new forms of content on mobiles[24] including the use of Internet services. The Code included a commitment to classify and restrict adult content to those over the age of 18 years. This means that Orange has placed all adult content (whether on our mobile Internet portal or the wider mobile Internet) behind access controls. The service prevents anyone under the age of 18 years from accessing adult content, whatever its source, while enabling them to surf the rest of the mobile Internet. An additional benefit is that all customers are prevented from accessing sites with illegal content as defined by the IWF.

2.11 In addition to this, Orange—again along with the other mobile operators—has also produced a separate Code of Practice to govern the use of passive location-specific services (ie using the mobile network to track or trace another person or asset). These services are strictly consent-based and comply with existing data protection legislation. The Code of Practice[25] supplements the legislation.

2.12 The growth and prevalence of the mobile Internet has also prompted Orange to develop and launch an anti-virus solution for handsets. To date we have launched an easy to install system, F-Secure, for all our Internet-enabled smartphones. The system is available as a download from Orange's mobile Internet portal and customers are protected from over 2000 viruses, worms and trojans. Future handsets will be sold with the latest software pre-installed and will be continually updated so that the customers remains protected.

2.13 The increase in mobile handset ownership in the UK and the ability to access the Internet from most handsets available today means that procedures must be in place in the event of the handset being lost and stolen. Orange's approach is therefore to make the SIM card and handset redundant when reported lost and stolen. This reduces the criminal's incentive to steal the handset in the first place and ensures that the customer's credit and personal information is protected in the event of theft. In 2002, Orange and the rest of the mobile phone industry implemented a system whereby a handset blocked on the Orange network will also be barred across all UK networks in the UK. Whilst a criminal will always target portable devices, such as mp3 players and mobile handsets, we believe this approach is helping to reduce street crime and personal robbery in the UK.

[23] Mobile Data Association: June 2006.
[24] www.orange.co.uk/about/regulatory_affairs.html
[25] www.orange.co.uk/about/regulatory_affairs.html

3. Consumer Information

3.1 Consumer advice is the heart of our strategy—both fixed and mobile—to help keep our customers secure online as well as keeping consumers aware of the potential dangers of the Internet, whether fixed or mobile. Our website includes a safety advice area offering advice to parents, carers and children. It includes the NetSmart guidelines written by the children's charity NCH and links to this area have been introduced across the communicate area of our website.[26] Orange promotes the Parent's Guide to the Internet, produced by the NCH, which seeks to educate parents about the Internet and how to help their children enjoy a safe and productive environment.

3.2 In the mobile space, Orange offers specific consumer information to assist parents or carers better understand the technology and what they can do to prevent children accessing inappropriate material using a mobile handset. This formed part of our commitment under the Code of Practice. As a result, Orange has produced a guide—available in retail outlets or online[27]—offering parents specific advice on a wide range of issues, including adult content, handset theft, passive location-specific services and bullying.

4. Is the Regulatory Framework for Internet Services Adequate?

4.1 Orange has implemented personal security features into its Internet services in conjunction with government, law enforcement agencies and children's charities. This self-regulatory and partnership approach has been welcomed by the Government and we believe it is the most effective way in ensuring regulation maintains pace with the technology and remains up-to-date. For example, UK mobile operators put in place the Code of Practice on new content prior to the mass take-up of Internet enabled mobile handsets.

4.2 We believe a more formal regulatory approach (ie via statutory legislation) would not necessarily achieve this and may not reach the right balance between the need for regulation, the freedom to enjoy the Internet and the development of innovative services.

4.3 However, this is a partnership approach and to this extent we do believe there is work the Government and Law Enforcement Agencies can do to help us ensure that our procedures are effective. Below we set out several ways that this can be achieved.

5. Recommendations

5.1 Orange believes the self-regulation of both fixed and mobile Internet services, in partnership with other key stakeholders, is the most appropriate method of protecting consumers from potential Internet dangers, whether personal or financial. We believe working closely with stakeholders—law enforcement, industry, government and consumer groups—is the best way of meeting the balance of achieving consumer protection whilst providing the flexibility to innovate and invest. Formal regulation would deny us this flexibility and would place at risk the benefits of many Internet services.

5.2 However, Orange believes there are areas where government and law enforcement can assist us in this approach, particularly in relation to consumer protection. In particular:

- We would like to see the Government bring forward legislation to make anonymous proxy servers illegal. In doing so, the Government would be greatly enhancing our investigative procedures in tackling consumer abuse on the Internet.
- We believe there should be greater clarity for the procedures in reporting suspicious Internet behaviour to law enforcement agencies and providing supporting information to assist cases. In doing so, this would ensure that, as an industry, we comply with the required legislation and support law enforcement effectively in their investigations, so assisting the partnership approach in tackling potential problems.

Memorandum by PAOGA

What is the nature of the security threat to private individuals and what is the scale of the problem?

PAOGA believes that the core of the security threat to private individuals centres around their Personal Identity. The loss of control of this data and the large number of databases in which this is held by Government and business makes fraudulent use of this data a very high risk. The current battle for control of our personal identity amounts to nothing less than a fight for the intellectual (?) health and social cohesion of our society.

[26] See www.orange.co.uk/communicate/safety/ .

[27] www.orange.co.uk/about/regulatory_affairs.html

We are, however unconsciously, in the midst of a collective identity crisis. Attacks on our personal identity are coming hard and fast from three distinct areas:

Loss of Privacy: Levels of scrutiny and intrusion into our private lives are spiralling out of control:

- Whether it be corporate spam, junk-mail, nuisance callers and phishing attacks, or the much more dramatic intrusions from the state (eg identity cards), the fact is that in more and more situations our lives are invaded and our integrity questioned. The onus is on the individual to prove who we are, how old we are, what we earn, and where we live—simply to earn the privilege of bombardment with information and interaction we do not want.
- Our organisational interactions leave a trail of data across organisational systems and the Internet which cannot easily be erased, leaving us increasingly powerless. Our physical location is almost permanently visible, through mobile phones, credit cards and traffic cameras. We have become easy to target by aggressors of all kinds.

Loss of Liberty: It is increasingly costly, time-consuming, inconvenient and downright frustrating to engage in everyday life:

- Our freedom to operate—to transact, and to maintain relationships is increasingly constrained by rules, regulations and procedures, ossified by government and corporate technologies that make it harder and harder for us to get what we want.
- From impenetrable telephone-based customer service systems, to the mandatory face-to-face interview for getting a passport, to the perils of driving down a motorway, to simply buying and selling a house, it's getting harder and more risky simply to go about our daily lives.
- Once again, it is our increasingly conflicted relationship with the state that poses the greatest risk.

Loss of Accountability: We lack any robust and reliable mechanisms for holding organisations to account for what they do with our information:

- Legal redress, peer pressure, management standards and good old fashioned ethics have so far been insufficient to persuade organisations to "do the right thing" with our information.
- Information about us is often incorrect; and even when correct it is too often lost, stolen or mislaid, or it is sold on legally or illegally—always without our knowledge, and always outside our control.
- Simultaneously, the state has ever more power to intervene in our lives without pause or redress, through tools like stop and search, on the spot fines, and extended detention. Meanwhile, corporations send debt collection agencies to your door with no means of recall.
- As individuals, we need a better mechanism for making institutions accountable for the ways they contribute to, and act upon our public identity.

What characterises all three threats is a fundamental shift in the burden of proof of identity, towards the individual. Organisations believe and act as if they, not we, control our identity. It is we, it seems, who must account to them, to prove who and what we are. The stark reality is that we have now lost all influence over what is known about us, how accurate that data is, what decisions are taken on the basis of that knowledge, how our reputation is affected, and critically, how our life options are eroded by its misuse. We have allowed our individuality to be outsourced.

These issues are of such great social concern that dedicated organisations and lobbying groups have identified themselves explicitly with these issues, namely: Privacy International, Liberty, and Accountability. The trouble is that as things stand these core aims are potentially in conflict. In order to protect our liberty, we are told we must give up privacy. And in order to safeguard our privacy, we must apparently sacrifice accountability. To participate in the modern economy we must tick boxes and sign forms to abrogate our rights to manage our own identity, on non-negotiable terms.

How well do the public understand the nature of the threat they face?

Individuals are only now waking up to the identity crisis. The fact is that most of us, as individuals couldn't, as yet, care less about these erosions. If they notice these incursions at all, they see them as an inconvenience. Our identity is abused by criminal networks and we just shrug. After all, what can we actually do? Until now, very little. Under the surface, though, the anxiety is building globally, and among affected groups the pain is already acute. In the UK alone, already:

- Almost 1 in 10 adults has had their identity compromised.
- More than 600,000 lost or stolen passports are in circulation.

— More than 500,000 driving licenses are lost or stolen—every year.

— More than 14 million households have signed up to the Telephone Preference Service.

The fact is, as a society we face a growing identity crisis. This crisis lies at the heart of our loss of trust. The old deferential models of trust are increasingly challenged.

According to a survey by Glasshouse Partnership in 2004, just 23% of the UK population would trust the Government not to abuse their data. But ask them if they'd trust Accenture or EDS to manage it, and just 5% agree. The lesson is: we trust no-one.

We cannot rely upon the state or corporations to manage our data. We must take charge for ourselves, as individuals. What is required is a totally new means of establishing, sharing and validating our human identity in a social context. We need a new space to build and share our identity, built around the individual and managed by them.

What can be done to provide greater personal Internet security?

The PAOGA approach to providing greater personal Internet security is to turn the existing system on its head. If we provide individuals with the tools to enable them to share their personal information and intentions safely and securely with their trusted partners, then all of this wasteful expenditure on security, customer surveillance and intrusion marketing can disappear. Billions of marketing dollars can be saved, to be diverted into genuine value-creating activities, like providing search and matching services that work on the individual's behalf.

Much more importantly, for the individual, the time-consuming and frustrating process of entering, updating, correcting and aligning data, validating and revalidating identity within relationships can be dramatically reduced. Instead of being imprisoned by our identity, it can set it free.

PAOGA believes that we must rebuild commercial structures around resilient networks of appropriately trusting individuals. Building an identity management eco-system that centres around the individual with dramatically increased accountability, privacy and liberty. Such a system will enhance social capital and mutual trust, and transaction costs will fall across the economy.

Rethinking the architecture of trust will also redefine the nature of the interface between the individual and the state. In a situation where individuals certify their own and one anothers' identity, individuals' service needs and entitlements can be accurately and uniquely targeted.

Every Utopian journey must start with a single step.

For PAOGA, that first step is to enable a new identity system which revolves around the individual.

How much does this depend on software and hardware manufacturers?

The resolution of these issues is dependent upon the IT Industry creating new Identity Management Standards and software developers creating interfaces within their applications to new Personal Identity Exchanges such as that developed by PAOGA. This will become the new identity architecture. The insights above have, of course, already spawned multi billion dollar businesses, and other smaller ones whose reach and influence are immense.

Looked at through an identity and individuality filter, we could argue that mySpace is a liberty engine—a giant marketplace of self-expression and projection. eBay is, of course simply a vast accountability system—a tool for trust-building and for direct reputation management.

Looked at from an identity standpoint, social networking tools like LinkedIn and Plaxo are actually privacy management tools—a tool for constructing self-image and analysing relationship capital.

But of course none of these systems remotely addresses the promise of fully-fledged identity management. All of them carry risks and trade-offs between liberty, privacy and accountability, and many of these trade-offs are still opaque to users.

From the analysis of the three identity threats and the corresponding responses to the Identity Crisis above, it follows that a better identity management system must have three key characteristics:

— Flexibility: It must enable the individual to express different facets of themselves (multiple personae) in different situations, and to enable rich information such as values, desires and needs to be shared, as well as facts.

— Control: It must enable the individual to protect, and analyse their information, including remaining anonymous in social situations so as not to compromise their true identity.

— Transparency: It must able to control the social context and rules under which individuals give out information, see what is done with that information, and benefit fairly from the value that the information creates.

In structural terms, the Copernican centre of the new identity system is the individual's Personal Knowledge Bank (PKB)—the secure and dynamic store of personal information individuals manage about themselves.

This enables the individual to police the accuracy of what others know about them, to express detailed needs, and help others to make more informed decisions about them.

Various Personal Information Management Services (PIMS) can orbit around this central data store and support analysis, storage and sharing of personal information with high security. Technologies like flickr and del.icio.us, and even iTunes are early precursors of this raft of services, but they do not, at present exploit the identity or trading potential of this personal content.

PAOGA is presently developing a portfolio of PIMS, which will enable individuals to share their data in different contexts where they may be identified or anonymous. This can include sharing address book information, creating CVs, managing their health and medical information. Other applications might include management of household information (suppliers and links to local authorities), and a range of financial services.

The planets in this analogy are Social Identity Marketplaces (or SIMs)—environments where personal information is applied in a social or commercial context to find tailored experience. Again SIMs exist already. Dating and matching sites like friends reunited, or permission-based marketing sites like myoffers.com are early SIMs but are insecure, and make little use of contextual information and the rich data stores that PIMs can produce.

The missing ingredients in this description are the laws of nature, including the force of gravity, which holds the solar system together. For individual-centric identity management to take off, individuals must be able to connect their information to others, knowing that those transactions are secure and that their underlying identity is not compromised.

PAOGA is supplying this missing gravity by building the first Person Identity Exchange (PIE) to allow individuals to conveniently & securely exchange their personal information, "under their control, with their consent, for their benefit", with other individuals, suppliers, and government.

All identity transactions between applications that use the exchange are facilitated through the PAOGA Push Protocol (an extension to WS-Security that provides for the highest levels of security). The identity exchange is a system that verifies the legitimacy of individuals while maintaining anonymity of their data. This is the equivalent of a stock exchange handshake. It uses the minimal amount of data to secure the highest possible level of trust in a transaction.

Beyond the core exchange functionality, PAOGA is developing a number of technologies which package identity data in different wrappers, for different trading situations.

Thus, for example, traders who wish to remain completely anonymous (for example high net worth individuals making high value bets) with one another can do so under the system. Equally, those who wish to transact with fully-validated and externally-certified data (for example employers and candidates) may do so.

The audit trail for all identity transactions will be transparent, and shared between the parties. Unusually, it will not just reflect the history of a transaction, but also specify its future, by proscribing the terms of use for the data. Finally, in line with its vision of reclaiming individual identity and rebuilding social trust, PAOGA will use the social connections. PAOGA is standing up for Privacy, Liberty and Accountability.

There is a better way. Now it's up to individuals to take action.

Is the regulatory framework for Internet services adequate?

The PAOGA experience of the regulatory framework around the Data Protection Act would lead us to conclude that this is not adequate to protect the individual in his interaction over the Internet.

Whilst compliance with the DPA is fairly high on the corporate list of responsibilities, when non-compliance is identified the Government Agencies tasked with monitoring and controlling the compliance find that the penalties available to them do not have any significant deterrent effect. The comment "When we get fined, we will do something about it" is frequently heard.

How well equipped is Government to combat cyber crime?

The evidence is very clear: Government is not equipped to combat cyber crime.

The recent incidents at DWP and DVLA where IT systems were hacked and the Personal Information of civil servants and the public have been removed and sold. If the Personal Information of the individual cannot be kept safe by Government then the trust between these parties is very much under threat.

This lack of trust places Government at a great disadvantage if it is to be seen by businesses as the leader for advice and action in dealing with this type of security threat in the future.

Is the legislative framework in UK criminal law adequate to meet this growing challenge?

We consider that more informed comment will come from those amongst us with a legal background.

Memorandum by ReadyTechnology

WHY PASSWORDS ARE BAD

Introduction

This article is directed at one specic aspect of personal Internet security that is the root of many other online problems—the password. While many other issues exist and deserve attention, the password is a fundamental issue that has been ignored for too long. If you just want a quick introduction to this issue, read the examples at the end, and then browse the rest of the evidence provided. It has long been known that passwords are not a secure way to authenticate an individual. However, most websites rely exclusively on passwords. Most users are unaware of the risks, or if they are aware of the risks, they use passwords anyway, because they have no choice. The evidence contained in this paper focuses on many of the issues relating to passwords—why they are not secure, why we still use them and what alternatives are available.

The author is an experienced software engineer and consultant. His main field of business is IP telephony. He obtained his degree in Computer Science from the University of Melbourne, and has first hand experience in helping businesses avoid security risks, recovering from security incidents, liaising with law enforcement authorities in the wake of security incidents, delivering training to IT professionals and designing and operating secure web sites on a daily basis.

Defining the Problem

What is the nature of the security threat to private individuals? What new threats and trends are emerging and how are they identified?

Passwords are a serious threat to the security of the private individual. A password can easily be used without the owner's knowledge, in much the same way as an untrustworthy tradesman might take a copy of a spare key and use it long after they've returned the original. The problems relating to passwords have been well known since the beginnings of the study of Computer Science in the 50s and 60s.

What is the scale of the problem? How are security breaches affecting the individual user detected and recorded?

The problem is immense—virtually all "e-commerce" web sites, including retail/shopping sites, telephone company sites, webmail services, banking sites, auction sites and online payment sites use the password as the sole means of authentication.

Recently, some banks have embraced more appropriate solutions, including digitalcertificates (which have the same level of security as the "Chip and PIN" system) and security "tokens"" which generate security numbers from a sequence that can not be predicted by a third party. Apart from a handful of banking web sites, virtually no other online service has moved beyond password authentication.

The very nature of the problem means that the web site operator is unaware that their site is being accessed by an unauthorised individual. It is rarely possible to detect. For instance, a person may read their spouse's emails for many months, and the spouse will never realise, as nothing has been changed or deleted.

If a password is misused for financial transactions, the victim may realise at the time they receive their next paper statement.

How well do users understand the nature of the threat?

A small percentage of the population understands the problem, probably less than 30%.

However, even amongst those of us who understand the problem, we have limited means of protecting ourselves.

An individual who understands the problem would prefer not to do business with any web site that relies only on passwords. This individual would quickly find that there are very few web sites they can use. Therefore, the user's understanding of the problem doesn't actually help them.

The operators of many e-commerce web sites are quite happy to continue providing services using passwords because the greater percentage of the population will simply use the service as it is, without questioning the security of their password. Many web site operators also feel that they need to make their service "easy to access" as this will increase their number of users and reduce the support costs. This means that the "easiest" solution is preferred over the "secure" solutions.

Tackling the Problem

What can and should be done to provide greater computer security to private individuals? What, if any, are the potential concerns and trade-offs?

Currently, the UK has a limited choice of schemes for online authentication of individuals. Most schemes are proprietary. For instance, HSBC bank issues digital certificates to it's own Business Internet Banking customers, including myself—these certificates are no use with any other online service. Under this arrangement, I would potentially have to keep a certificate for every one of 50 web sites I log in to—a real nightmare for myself, and impossible for someone who's knowledge of computer security is minimal.

A preferable solution would involve a common certificate that could be used with any of the banks and other interesting web sites. The end user would only need a single certificate, no matter how many online services they wished to access. They could store this certificate on a single card, and carry it in their wallet.

The trade-off is that the individual can only access the secured websites from a computer which has a "smart card" reader. This is not a significant challenge, as inexpensive "pocket sized" readers can be carried and easily fitted to the USB port of a PC.

Another trade-off is that the user who loses or "blocks" their certificate (by damaging the card or incorrectly entering their PIN three times) will be unable to access any secured web site for a period of several days while awaiting a replacement card/certificate.

One way to encourage this type of scheme (which should be run by the private sector, but to a standard endorsed by Government) would be to provide a security rating for "e-commerce" web sites. Businesses which trade online would need to satisfy certain criteria, including the use of strong authentication (something better than a password), in order to get the security rating. Just as consumers understand the ratings of movies, they could be educated to recognise the security ratings of web sites.

What is the level of public awareness of the threat to computer security and how effective are current initiatives in changing attitudes and raising that awareness?

The public is vaguely aware that computers have risks associated with them. However, people have bad habits (eg they often trust what they see in print, even on a web site) and they take risks—for instance, they are so keen to check if they have new email, that they will risk typing their password into an untrustworthy computer that may have a keystroke logger/spy software fitted.

People are so concerned with enjoying the benefits offered by the Internet, that they seldom take time to understand the risks.

Most motorists are probably not familiar with all the risks of driving their vehicle. Fortunately, MOT testing and regular services allow the motorist to drive with relative safety, oblivious to many issues that they might otherwise experience. In the computing industry, however, "security" products are often limited, mis-used and sold with profit as the main motive, and public interest as a minor consequence. Users who buy this software often find themselves nagged by constant reminders to "upgrade" (which has a price tag), so they often give upon the software after only a few weeks or months.

What factors may prevent private individuals from following appropriate security practices?

Many individuals are under a great deal of pressure to do many things during their day. When they only have five minutes available to check their email, they will not be thinking about "how do I check if this PC has spyware", they will just go straight to the web mail site—and type their password.

Furthermore, the fact that passwords are used as the standard means of authentication on so many sites means that many users who are unfamiliar with the risks will have a false sense of confidence in this form of security. Few web sites have a warning message on their login screen advising the user to "please check for a keystroke logger before entering your password".

It is often said that users should:

— Use a different password for every every web site/computer that they access.
— Change every password regularly.
— Never write down their password(s).

It's clear that with so many websites in popular use, the average member ofthe public can not easily practice all these rules. The average person may have to remember over 20 passwords—or carry a list of them all in their pocket. They need their bank password, their webmail password, their online phone bill password (for both their landline and mobile provider), their broadband password, their Wireless/Wifi network password, their auction password (eg eBay), a password for the computer system at their office and many more. Given all these passwords, the user will simply choose the easy option—using the same password for every site.

What role do software and hardware design play in reducing the risk posed by security breaches? How much attention is paid to security in the design of new computer-based products?

Everyone is basically avoiding any responsibility—if they are even aware they have a responsibility. I recently met someone who had a degree in computer engineering and was oblivious to the issues relating to passwords. While Oxford and Cambridge are producing some very talented IT professionals, the vast majority of small business IT and computer systems, and websites, are produced by people with minimal knowledge ofsecurity issues. As the education sector rushes to provide greater and greater quantities of "work ready" graduates, they neglect issues relating to security and focus on specific hands on training in technologies that are in common use. This new class of graduate has been shown how to build web sites with "point and click" rather than with essential theory of computer security.

Small business budgets often mean choosing the cheapest security option when designing a web site—passwords.

Many software developers who are aware of the risks posed by passwords are afraid to stick their neck out, or they are satisfied to just give their boss the insecure password based system that he asked for. Avoiding controversy, they can get the job done more quickly and collect their pay cheque.

Modern PC hardware and the most common PC operating system provides the user with little assurance that their keystrokes are truly private. However, it only costs £15 to attach a smart card reader to the PC's USB socket. The PC can then easily and securely perform authentication tasks using secure digital certificates.

Who should be responsible for ensuring effective protection from current and emerging threats?

The providers of online services have a significant role to play, particularly the banks and popular online webmail services. Were they to set standards for online security, smaller businesses and web site operators would then follow suit, for two reasons:

— because they would have an example to follow, and would not want to appear "behind the times" or careless about security; and
— because individuals would become more aware of the stronger means of authentication offered by digital certificates, and many individuals would then become reluctant to engage with web sites not supporting that type of security.

What is the standing of UK research in this area?

The issue is well beyond the point of "research". Practical solutions already exist, and are used already in niche sectors or proprietary systems. For instance, "Chip and PIN" has already been implemented successfully for cash machines and in-store payments—it simply needs to be brought to the Internet.

Governance and Regulation

How effective are initiatives on IT governance in reducing security threats?

In the case of passwords, governance has not yet played a part. Government could play a role in several ways:

- By example—using certificate based security for all e-Government services, exclusively, and refusing to procure from any supplier who relies on a password based web site.
- By setting rules or endorsing standards—for instance, a standard that all "e-commerce" web sites must meet for user authentication.
- By focusing on "high-risk" sectors that are already regulated—for instance, finance. Financial institutions have chosen to make their web sites "easy" rather than completely "secure", as they want to increase the number of customers who use the site, and reduce the cost of providing technical assistance to customers. They have chosen to give customers services that are "convenient for the masses" rather than services that are secure. As these institutions are regulated and licensed, they could potentially be directed to improve their performance in this area, with or without specific regulations. If a customer is unable to understand the security technology, then it probably isn't appropriate for the bank to be forcing that customer online in the first place.

How far do improvements in governance and regulation depend on international co-operation?

The standards for digital certificates already exist on an international basis. Numerous products in this field are already marketed internationally.

Is the regulatory framework for Internet services adequate?

It is adequate for punishing people after something goes wrong. However, it doesn't create the impetus for businesses to tighten up their web site security.

What, if any, are the barriers to developing information security systems and standards and how can they be overcome?

There are several barriers:

- Different levels of understanding within the IT community—many IT people are simply happy producing the web sites and systems that they get paid for. They won't change their practices unless there is a strong commercial reason for them to do so.
- Many businesses simply trust the advice of their IT staff or consultants, without testing that advice. Businesses need to have independently specified standards that they can rely on when they give direction to their IT staff/consultants/web developers. If a business decision maker doesn't know what to ask for, he will usually be given a solution that is not particularly secure.
- Co-operation between businesses—businesses who operate online need to be willing to trust one or more common "certificate authorities" who issue digital certificates to private individuals. However, this is not a major challenge, as the certificate authorities already provide SSL certificates to many web sites.

Examples of Password Abuse

The information presented here is not intended to be performed or duplicated by the person reading this document. This information is presented in the hope of educating the public about the risks of passwords.

Keystroke Logger Hardware

A keystroke logger is a small piece of hardware that is attached to the keyboard cable. It records every key stroke pressed and released. The person who controls the device is able to retrieve a log of all the keystrokes since the device was fitted.

Example usage:

- Purchase keystroke logger from web site or online auction.
- Select a PC that will be used by the intended victim.
- Detach the keyboard.

— Attach the keystroke logger to the keyboard cable.
— Attach the keystroke logger to the PC.
— Allow the victim to perform their usual tasks, eg accessing email.
— When the victim is gone, remove the keystroke logger.
— Attach the keystroke logger to another computer.
— Install the software for readingthe log.
— Review the list of keystrokes on the screen. Identify usernames and passwords.
— Use the passwords to gain access to the victim's email, etc.

Analysis

It should be obvious that the above procedure requires no special training or signicant technical understanding.

Keystroke Logger Software

Keystroke logger software operates in a similar way to the hardware device. The software is installed on the computer by the perpetrator. They can then use another computer, anywhere on the Internet, to see what is on their victim's screen, and to see which keys the victim is pressing.

The procedure is as follows:

— Obtain keystroke logger/screen grabber software.
— Install the software on victim's computer, or a computer the victim is likely to use.
— Make a note of the IP address of the victim's computer.
— Install the monitoring software on another computer.
— Run the monitoring software, and specify the victim's IP address.
— The monitoring software will display the victim's current screen and keystrokes as they take place. It may also allow the victim's keystroke history to be inspected.

The use of the keystroke logger/screen grabber software is a superior alternative to the hardware logger, for the following reasons:

— The screen can be viewed—this means that security systems that require the user to "click" a number can also be breached.
— It is not necessary to return to the victim's PC to retrieve data.
— Data can be accessed in "real time"—while the victim is using the PC, instead of afterwards.

Analysis

The software for committing such crimes is easily obtainable online. It can then be carried around on a CDROM or "pen" drive.

The victim may be able to protect themselves by using a secure BIOS, secure operating system (eg UNIX) and requiring a password to be entered by anyone who installs new software.

Web Site Example

World Wide Widgets Ltd (a fictitious name, we will refer to them as WWWidgets) sells widgets through their web site.

Wendy works for WWWidgets, maintaining their website and database.

Wayne, a customer, creates an account on WWWidgets' web site.

He chooses a password—the password is transmitted securely to WWWidgets using SSL. The SSL encryption ensures that no eavesdropper is able to see the password while it passes through the Internet company's network.

The password is received and stored, without encryption, in the database designed by Wendy.

Wicked (that is not his real name, but his "screen name") breaks into WWWidgets' office and steals their computer. After all, it is easier to break into a small company than a bank.

Wicked finds Wayne's email address and password in the database. Wicked uses this information to access a well-known online payment service, where he purchases £500 of goods from online stores, using Wayne's credit card details. Wicked finds that he is able to de-fraud over 1,000 people in this way, using passwords from WWWidgets' database.

It takes WWWidgets four days to realise the risk to their customers, and another seven days of internal management debates before they decide to warn customers. By this time, Wicked is untraceable.

Analysis

Wayne was at fault: he used the same password on the WWWidgets site and the online payment company's web site.

Wendy was also at fault: she stored the passwords without encryption. Using an algorithm such as MD5 to encrypt passwords would have made Wicked's work much harder or impossible.

The online payment service is at fault: they accept the password as the single method of authentication, and then allow the user having the password to execute transactions using stored credit card or direct debit details.

Conclusion

The information here will hopefully contribute to public understanding of the risks posed by the use of passwords for online authentication.

Passwords are the root cause of many other problems in computer fraud, including the practice known as "phishing". Obtaining passwords and/or credit card numbers (which are also disgracefully vulnerable) are some of the main reasons for hacking or stealing computer equipment.

If no physical trespass has occurred, then it is possible that the theft of passwords may not be detected until long after subsequent crimes and abuses of privacy have been committed.

21 October 2006

Memorandum by Research Councils UK (RCUK)

Introduction

1. Research Councils UK (RCUK) is a strategic partnership that champions the research supported by the eight UK Research Councils. Through RCUK the Research Councils are creating a common framework for research, training and knowledge transfer.

2. This memorandum is submitted by RCUK and represents our independent views. It does not include, or necessarily reflect the views of, the Office of Science and Innovation (OSI). RCUK welcomes the opportunity to respond to this inquiry by the House of Lords Science and Technology Committee[28] and provides evidence from RCUK in response to the main topics and questions identified in the consultation document.

3. RCUK asks the Science and Technology Committee to note the following:

- The Council for the Central Laboratory of the Research Councils (CCLRC) is responding in its capacity as technical advisors and not in its capacity as a legal council. As an employer, CCLRC has consulted on the aspects of employees using the Internet at home as private individuals.
- In relation to EPSRC, much of the work involved in defining the problem either falls in the domain of private companies, or research into social issues which are covered by other Research Councils. Undoubtedly, many of the researchers funded by EPSRC will be engaged with those defining the problem, but they will be using this as a driver for research. This, in itself, is not led by EPSRC and as a result the impact of that understanding is only seen second-hand in the form of research grant applications around solution technologies.

[28] http://www.parliament.uk/parliamentary_committees/lords_s_t_select/internet.cfm

Defining the Problem

4. There are many different reasons why private individuals use the Internet. This may be choice, neccesity, interest, reference, companionship, shopping etc. A common factor is that individuals increasingly trust Internet based services. On the whole, society now regards Internet access and Internet services as "normal", not just for IT experts. While most individuals are concerned about their personal security they do not understand how to assess IT security risks. They do not wish to become IT security experts, so that they can make informed judgments, they just want the Internet to work safely.

What is the nature of the security threat to private individuals? What new threats and trends are emerging and how are they identified?

5. In broad terms, the threats to individuals from the Internet and Internet services can be grouped as "technical" and "non-technical".

Technical threats

6. While most individuals are aware that technical threats, such as computer viruses, worms or spyware exist, they are not aware of how they pose a direct or indirect threat to them. The vast majority of individuals do not wish to, or need to, understand how these technical threats work. Often they are only aware of the threat once it has resulted in some destructive or invasive activity on their own personal computer-based device(s).

7. Organisations and Companies are usually more aware of technical threats as these pose a higher risk to their day to day operations. As such, they have usually taken advice from IT professionals or security experts to reduce this exposure by:

- Keeping computer systems up-to-date with security fixes.
- Installing computer anti-virus software.
- Using a "Firewall" between the organisation and the Internet.
- Issuing individuals with usernames and passwords to audit use.

If implemented correctly, these techniques can vastly reduce the level of technical risks to organisations and the individuals within them.

8. Individuals care about security. Good experiences from within organisations such as work, school, college etc. have resulted in many individuals developing the perception that the "internet is safe". However, as the individuals are not IT security experts they lack the skills to understand the steps taken by organisations to protect themselves and find it difficult to privately implement technical solutions. They often see them as too technical; too costly (eg not free); too cumbersome or irrelevant. The language and terminology used by IT security experts is inaccessible to most. This lack of IT security understanding effectively forces individuals to accept a higher personal risk when using the Internet from home. Some organisations provide advice on home computer use to their employees, particularly if the home computer is used partly or wholly for purposes associated with employment.

9. Technical threats are relatively mature, well known and understood within computing environments. Individuals may have heard of the following simple categories based on how systems are impacted:

- virus—(infection comes via a floppy disk, software or e-mail);
- worm—(can spread by itself—the infection does not need a host);
- spyware—(sends information to a third party without the individual's permission or knowledge); and
- port scanning—(an individual attempts to gain access to your computer);

but do not know or care about how to distinguish a computer "virus" from "spyware".

10. Recently no new major categories of technical threats have emerged but some manufactures are starting to use the term "malware" to include all viruses, worms and spyware. The trend of combining the characteristics of basic technical threats to construct "hybrid" or "blended" attacks continues with an attendant increase in technical sophistication, level of automation and speed of attack. In addition, the time taken to develop and issue new attacks is decreasing.

11. E-mail remains the major method of attack against individuals due to high level of unsolicited e-mail (or "spam") which if read or respond to, can install unwanted software (or "malware") on their systems. The malware may be downloaded from a website referred to in the spam message or attached to the message. Once

installed, the malware can cause direct or indirect harm to the individual. Port scanning that could result in an attacker finding access to system administrator functions and thence control of the machine is also on the increase.

Non-technical threats

12. By the very nature of the Internet, it brings individuals into contact with many others faster and potentially across greater social and physical distance than traditional media for communication. What one individual finds "interesting" can be perceived as a threat by another. The lack of physical clues and social signals can also prevent individuals avoiding unwanted contact.

13. As with all human endeavours, a minority of individuals are motivated by criminal gain to find ways to abuse systems and services that the majority trust. This abuse can be targeted against private individuals or organisations and can either be direct or indirect. In the context of accessing the Internet or Internet services, it is important to remember that this criminal activity is not dependent on any technical means. Criminal activity is very much a business (with questionable motives) that will "follow the money" and will attempt to exploit private individuals. The Internet is now used by sufficiently many private individuals for some criminal activities to be cost effective.

14. Most, if not all, individuals who use the Internet, initially trust it. They may hear of technical threats (such as viruses) and non-technical threats (such as "phishing") but unless they are directly or indirectly affected by these, they may believe that these "happen to others". The Internet does not add any new fundamental risk to individuals within society. However, the sheer scale, diversity and inherent trust in the Internet and services offered by it can be abused resulting in:

- Theft (eg money taken from bank account).
- Fraud (eg buying or selling items that you do not have or own).
- Impersonation (eg "identity theft").
- Deception (eg obtain information by pretending to be a bank—"phishing").
- Extortion (eg threatening to disclose information about activities on the Internet).
- Abuse (eg exposure to offensive images).
- Defamation (eg wrongly accused of an act).
- Invasion of privacy (eg unwarranted access in to private matters).

15. Recently the activity known as "phishing", which is a blended attack where individuals are deceived into revealing private information that can be used to impersonate them within the Internet, has been increasing. This often results in direct financial loss or theft.

16. All of these non-technical threats exist in the "real" non-Internet world but individuals have learned ways to judge and manage these. For example, individuals are advised by banks not to lose their Personal Identification Number (PIN) when they use cash machines or pay for goods in shops. They routinely try to physically shield or secure the entry of PINs on shop keypads so that onlookers (including staff) cannot see it and use it. They know that not doing this could result in them losing money.

17. If individuals assume that purchasing goods via the Internet is just as safe as in a physical shop or store they will not have the physical clues that can help validate this assumption. Some individuals may be unable to judge how to replace these physical clues with appropriate Internet clues. An example may be the use of the HTTPS protocol to protect purchases via the Internet—the equivalent of shielding a PIN number in a shop. The use of the HTTPS protocol on its own does not guarantee that the web site is genuine. For example, the individual may not be buying from a genuine merchant.

18. Some of the physical and emotional clues used to prevent other forms of abuse such as fraud or extortion, develop as individuals mature. A lack of social awareness can make some individuals more vulnerable to some of the non technical threats. It is unsafe to generalise and state that "younger or older individuals are at more risk".

What is the scale of the problem? How re security breaches affecting the individual user detected and recorded?

19. On an annual basis, the number of technical threats is continuing to grow steadily at approximately 1,000 per month (from July 2002 to December 2005 the estimated number of distinct viruses grew from approximately 75,000 to 115,000). While some new viruses and worms have caused short term dramatic increases in this number, the impact on individuals who use anti-virus products has been less dramatic.

20. Non-technical threats such as distinct phishing web-sites are also increasing steadily at approximately 800 per month. (Between July 2005 and 2006, the number of phishing web sites increased from 5,654 to 14,191). These evolve rapidly and attempt to trick individuals into giving access to information or resources that can harm them. While IT security companies can help, they are always reactive to these new threats and the impact to individuals is increasing.

How well do users understand the nature of the threat?

21. Individuals are concerned by the threats but do not understand them. Intuitively they know they wish to be protected but do not know how to assess possible solutions.

Tackling the Problem

What can and should be done to provide greater computer security to private individuals? What, if any, are the potential concerns and trade-offs?

22. The Research Councils would welcome the outcome of the report which may identify the research challenges facing this area.

23. The UK has a very strong Information and Communications Technology Research Community, and the underpinning research into both hardware and software is of a high international standing. EPSRC's research projects have been funded mainly through their responsive mode route, but are also in response to calls for proposals from the EPSRC Crime Programme. Although providing a focus for research related to crime, the Programme has not had a call specifically targeted at Personal Internet Security. The projects supported span a range of technologies and approaches, from understanding the threat from a system perspective, through to profiling of the activities of criminals on the web. Many of the aspects of tackling the problem will be closely linked with understanding human behaviours and social interactions. Many of the EPSRC funded projects involve social science collaboration, however a major proportion of social science research in this area is funded by ESRC such as the various projects on Privacy and Trust under the ESRC e-Society Research Programme.

What is the level of public awareness of the threat to computer security and how effective are current initiatives in changing attitudes and raising that awareness?

24. Clearly this is an area of importance and risk, both real and perceived, to the public. EPSRC is currently engaging with its Societal Impacts Panel to identify ways in which the research community in the ICT area can engage with the public to identify the issues, and any research challenges associated with them. In addition, ESRC is working with the Technology Strategy Board on a proposed call relevant to human factors in network security.

25. Individuals believe that the Internet Service Providers (ISPs) that provide access to the Internet in private homes should take some responsibility in providing a "safe" service. This could be take the form of:

- "free" access to technical tools that can stop known threats (eg worms, SPAM and viruses) from being sent to individuals;
- having a system that automatically protects individuals from known attacks (eg TCP port scanning or access to phishing web sites);
- schemes such as the Central Sponsor for Information Assurance (CSIA), CSIA Claims Tested (CCT) kite mark could be extended to allow ISPs to demonstrate a commitment to protect individuals by agreed means; and
- a tax incentive for ISPs to participate in the agreed kite mark scheme.

26. "Free" to an individual includes not needing to know how the service works, just that it is active, current and effective. ISPs may wish to charge for this "safe" service but this is likely to discourage individuals. It may be more effective if ISPs received a tax incentive for participation in any such "safe" service.

27. Individuals may wish to use digital certificates to help increase their confidence in the on-line identity of others they deal with. This could include major websites, government organisations and banks. To gain any real benefit, this would require significant participation by a large number of individuals and organisations and would be unlikely to succeed if it was costly or required technical intervention by the individuals. Existing commercial and Government infrastructures could be expanded to form a national trust framework supporting the authentication and authorisation of individuals and organisations.

What factors may prevent private individuals from following appropriate security practices?

28. Individuals are aware that good security practice is in their interest. Often they just do not understand it. It is very difficult, if not impossible, to produce generalised accessible good security practices information that individuals wish to find and act on.

29. Some individuals are aware of on-line resources such as the Government IT Safe web site (http://www.itsafe.gov.uk/) and may purchase third party add on security products such as anti-virus software etc. As a society we have been led to believe that we must have access to the Internet 24/7 but few are prepared to pay for a renewable annual subscription to these "additional" services.

What role do software and hardware design play in reducing the risk posed by security breaches? How much attention is paid to security in the design of new computer-based products?

30. While it is possible for manufacturers to improve how their products work so that the risk to individuals is reduced, this is unlikely to happen on a national scale unless there is a clear financial gain or deterrent. A voluntary standards based approach (such as an extended CISA CCT scheme) may allow some to develop a market to attract new customers, but again this is unlikely to succeed if individuals do not get the benefits for free.

Who should be responsible for ensuring effective protection from current and emerging threats?

31. Manufacturers could take steps to improve the way their products work and reduce some of the exposure to individuals. This may benefit some market sectors and damage others. ISPs could pre-filter and control Internet traffic but some individuals may see this as a loss of privacy and a right to free speech. Ultimately individuals are responsible for their own actions, but care is needed to provide for the safety of vulnerable populations, especially children.

What is the standing of UK research in this area?

32. While the UK does not specifically have a leading reputation for academic research on IT Security, there are some outstanding institutions that specialise in this and related fields. A number of UK companies have developed an authoritative reputation for advice. However UK does have a very strong position in research on trust and human computer interaction which could lead progressively to more flexible, understandable and safe protections systems.

33. As mentioned previously, ESRC are in discussions with the technology Strategy Board about various collaborative opportunities between researchers and business relating to Network Security which clear strongly relates to issues around computer security. This would include investigating both technological and non-technological vulnerabilities in systems, how they are used and implemented. This kind of initiative will draw in researchers from related areas to look at these and therefore develop research capacity in the field by utilising existing capacity in related area of research.

Governance and regulation

34. Governance and regulation are issues generally considered at the development stage and by business more generally. EPSRC does not hold a position on governance and regulation, although ESRC funds a number of projects which have clear regulatory and governance relevance.

How effective are initiatives on IT governance in reducing security threats?

35. Current IT Governance initiatives are largely targeted towards organisations and not individuals. They require IT Security skills and funding to implement. As such, they have had little or no impact on private individuals. Given this it may be considered that thereare several anti-groomimg paedophilia initiatives which could be considered as making some head-way although the question asked here appear to look at financial threats not grooming. Since individuals may be committing offences in regard to the intellectual property rights of companies and artists this may be considered relevant in tackling criminal threats involving the specific use of these technologies.

How far do improvements in governance and regulation depend on international co-operation?

36. The Internet does not recognise national or state boundaries. Regulation within any state can be bypassed unless there are strong enforceable international agreements between states. A topical example of this is Online Gambling, which is illegal in some countries and not others.

Is the regulatory framework for Internet services adequate?

37. The current UK regulatory framework for ISPs is adequate but would benefit from additional guidance and enforcement and should be regularly revisited to account for new developments.

What, if any, are the barriers to developing information security systems and standards and how can they be overcome?

38. While some organisations use international standards for the management of IT security (ISO/IEC 27001:2005), these are not generally applicable to personal use of the Internet. A barrier to this is the potential for moral hazards. Organisations find achieving this standard complex, time consuming and costly with little visible return on investment.

Crime Prevention

39. EPSRC provides a raft of underpinning research which may be used in the prevention of crime in this area, but is more usually exploited further down the development chain. There are occasional examples of specific research in this area (eg "Detecting and Preventing Criminal Activities on the Internet"—Professor D Parish, Loughborough), but as before these are either in response to a generic crime call or through open responsive mode.

How effective is Government crime prevention policy in this area? Are enforcement agencies adequately equipped to tackle these threats?

40. Individuals who have suffered direct loss usually wish that the perpetrator is prosecuted in some way, although the individual's first concern is that they should suffer no loss rather than that criminals will be prosecuted. Often with computer damage or crime and individuals feel that UK enforcement agencies are not coping with these threats. The inability to prosecute individuals after apparently tracing them is seen by many as a failure of the system. Again individuals lack the legal and IT Security skills to realise how difficult this apparently simple task can be.

Is the legislative framework in UK criminal law adequate to meet the challenge of cyber-crime?

41. CCLRC is unable to comment on how effective the legislative framework in the UK is in challenging cyber-crime. In 2004, the All Party Parliamentary Internet Group reported on the possible revision of the Computer Misuse Act 2000. Although the ESRC does not hold opinions directly on the standard of legislative frameworks they do support researchers which clearly play a role in considering and addressing such issues and challenges. For example, ESRC fund researcher in International Relations, Socio-legal studies and Criminology (AHRC funds research into Law).

How effective does the UK participate in international actions on cyber-crime?

42. RCUK is unable to comment on how effectively the UK participates in international actions on cyber-crime.

Memorandum by the Royal Academy of Engineering

Defining the Problem

1. *What is the nature of the security threat to private individuals? What new threats and trends are emerging and how are they identified?*

1.1 There are a number of threats to individuals' security on the Internet. Very generally these fall into two categories: attackers gaining access to information that they should not; and attackers having control over computer systems that they should not have access to.

1.2 The largest single threat to private individuals comes from those attempting to gain access to personal information in order to use this information for fraud. The most common type of attack in this class is known as "phishing", in which a user is tricked into divulging confidential information such as bank account details to a third party (typically by getting an email supposedly from a bank, which asks them to go to a webpage and enter passwords and other details). The goal of a phishing attack is usually to enable either direct fraud or more general identity theft. By gaining access to private, personal information, bank accounts may be accessed, loans obtained in the name of the victim or documents obtained to further longer term fraud. The same techniques for gaining personal information may also be used for other types of privacy violation including stalking.

1.3 Another common route for gaining access to an individual's personal information is to gain access to that user's computer. If the attacker can install a program onto the user's computer, either by means of a computer virus or by having the user accept a "trojan horse" program[29], then the attacker may misuse the computer in a number of ways. The program may be used to send details of the user and information about their user names and passwords for web sites back to the attacker. The program may also enable the attacker to use the computer as a "zombie", remotely using the computer for further malicious purposes. This may include commanding the computer to send out junk advertising email; using it to spread viruses; or using it, alongside many other computers, to access a particular server in order to overwhelm it in a "Denial of Service" attack.[30]

1.4 The use by home users of always-on broadband and wireless Internet increases the risk of malicious companies or persons gaining access to computers owned by private individuals.

2. *What is the scale of the problem? How are security breaches affecting the individual user detected and recorded?*

2.1 Reliable figures for the scale of the problem are hard to come by, for three major reasons. First, most reporting on the problems comes from companies in the business of selling tools to help combat the problems, so it is possible that the figures are exaggerated. Second, figures for the level of fraud resulting from illicit computer access are even harder to come by, since banks are unwilling to admit liability and frequently deny that customer accounts could be compromised without the complicity of the customer. Third, evidence of an attempted attack is usually only found by exploring a computer system, and in many cases it is likely that most users live in ignorance of security breaches until, say, a false transaction appears on a credit card statement.

2.2 Despite these difficulties, some judgements can and have been made about the levels of threat. It is obvious to most Internet users that phishing email scams have reached epidemic proportions. Many users receive multiple phishing emails each week. With regard to the level of infection with trojan programs, the numbers vary by region but a recent survey put the rate above 30% of Windows PCs (though a caveat applies here, as this report was produced by a company with a business interest in this area).[31]

3. *How well do users understand the nature of the threat?*

3.1 Most users are aware that there is a problem but few are aware of the detailed nature of the threat. Phishing scams are confidence tricks and any success they have is due to a lack of detailed understanding of the threat. Phishing scams have become increasingly sophisticated, since making a convincing fake bank website is quite easy: the attacker can simply make a digital copy of a genuine site. Individual users need to be alert to

[29] A malicious programme disguised as, or hidden within, legitimate software. A trojan can be contrasted with a virus in that a "virus" is malicious code that is attached to an otherwise bone fide program or file, whilst a "trojan horse" is software that purports to provide useful functionality, but has deliberately been designed to include malicious code.

[30] Denial of Service (DOS) attacks usually target high-profile websites, seeking to bring them down by overwhelming the server that hosts them. Threats of such attacks have, in the past, been the basis of blackmail cases.

[31] http://www.webroot.com/resources/stateofspyware/excerpt.html

the small details to know that a site is one created by a fraudster rather than a legitimate site. However, many banks and online vendors publicise warnings about phishing scams and give customers information on how to identify and avoid them.

Tackling the Problem

4. *What can and should be done to provide greater computer security to private individuals? What, if any, are the potential concerns and trade-offs?*

4.1 One valuable way to help private individuals is to provide them with more information about what they receive, and what they are asked to download or run on their computers. This will enable them to make more intelligent decisions. The Oxford Internet Institute (OII) has a project entitled Stop Badware[32] that seeks to do this. The website points out programs, such as screensavers and anti-spyware software, that in fact include spyware or other "malware" that can be used to "spy" on a computer (eg, check which Internet sites its user visits, or spy on keystrokes to find passwords), or interfere in its running. The aim is to inform and empower users so that they do not compromise the security of their computers by downloading such software. Projects such as this serve a useful purpose, but require support and funding to function.

4.2 However, while it is possible to seek to mitigate against the effects of "trojan horses" by publishing lists that identify the software concerned, this is not possible in the case of viruses. Aside from not downloading any executable files, the key mitigation available to an individual to combat viruses is the use of up to date antivirus software. The installation and use of firewalls on PCs is also of great value in protecting individuals from various threats.

4.3 Computer system vendors would do well to spend more time thinking about how to allow the user to make informed decisions, with effort in the areas of user interface design and mechanisms that let the user ensure that they are talking to the correct web site. However, those in the computer security product business have a vested interest in selling things. There is already evidence of various false alarms from one or more of the vendors. Therefore, independent sites like Stop Badware may be more helpful. There is also a need to keep educating users to ensure that they always download the latest security patches for their operating system and the latest updates for any antivirus software that they are using.

4.4 In addition to informing users, much more could be done to make computer operating systems less vulnerable to viruses and malicious code that can be installed without the users' knowledge. Windows is particularly vulnerable to malware, whereas other operating systems such as Linux and MacOS tend to be less vulnerable—though they are not free from vulnerabilities.

5. *What is the level of public awareness of the threat to computer security and how effective are current initiatives in changing attitudes and raising that awareness?*

5.1 The Oxford Internet Surveys (OxIS) are tracking public uses and opinions about the Internet and have information relevant to the level of public awareness and concern. They reveal that most users are aware of threats, and most users have done something to address their concerns. For example, when asked: "How concerned are you about protecting your computer from viruses?", only 12% of users said they were "not concerned". 65% said they were "concerned and have done something" to address it. These statistics are presented in the report *The Internet in Britain: The Oxford Internet Survey (OxIS)*.

5.2 However, despite fairly high levels of awareness and concern about threats in general, the level of awareness of the actual threats is fairly low. Scare stories from parties with vested interests are widely reported by the press with over-simplification and sensationalism in reporting sacrificing the accuracy of the reports. Balanced and informative coverage of the issue is often judged too technical to be widely reported. As a result many people are worried about spurious threats while being ignorant of the real problems.

5.3 For those who have some awareness, there are various resources on the Internet but care is required because of the vendor self interest. Initiatives like Stop Badware could be useful for raising public awareness, as could the Government-run "Get Safe Online" initiative. However, these need significant publicity in order for the wider public to benefit from them.

[32] see http://stopbadware.org

6. *What factors may prevent private individuals from following appropriate security practices?*

6.1 There are two main factors that hinder individuals' adherence to security procedures: ignorance and haste. When presented with a security critical decision, for example, when a pop-up box appears before downloading a program, many users view it as an obstacle to the download and simply click "OK". However, if the user was aware of the significance of the decision they may be less hasty. If the computer systems presented the security questions to the user in a more understandable manner, explaining the risks that the user takes in downloading a program, and if users were better educated as to the impact of making the wrong choice, then users would be more likely to follow appropriate security practices.

7. *What role do software and hardware design play in reducing the risk posed by security breaches? How much attention is paid to security in the design of new computer-based products?*

7.1 Engineers of all disciplineshave a duty to ensure that their systems are "fit for purpose". The concern is that, currently, some computer software is not "fit for purpose" with respect to issues of personal security. Therefore, better software, both at the operating system level and at the application level, would be hugely helpful in addressing this. For example, trojan horse code derives its power from the poor level of separation of functional roles on most personal computers. Operating systems which better separate functional roles would give a degree of damage limitation in the face of trojan code. Computer viruses propagate through weaknesses/bugs in the operating system. Fixing the bugs, or building systems with fewer bugs in the first place, would slow the propagation of viruses.

7.2 Hardware security devices can also be helpful for personal computers, though only with the co-operation of the software. Trusted Platform Modules (TPMs—modules that enhance security by cryptographically scrambling and controlling access to messages and stored data) are starting to appear on personal computers and these can, in theory, help with protecting user data but ultimately it is the software that is the critical factor.

7.3 Another possibility is the development of system designs and products that manage machines remotely for retail users. This remote management is normal practice for most corporations. Such remote management can ensure that all the patches that have been developed to combat known vulnerabilities of the computer operating system and software applications have been installed, that up to date antivirus software is in place, and that the traffic flowing to and from the computer is under the control of an appropriately configured firewall.

7.4 Developments could be made to the design of access to websites such as banking websites, to prevent phishing attacks. An interesting example can be found on http://www.tricerion.com/. On this website Tricerion present a demonstration of a log-in procedure designed to prevent phishing attacks. They have incorporated a number of features into the login procedure, for example, presenting the characters of a user's password on a keypad displayed on the computer screen, which the users click on. This means that any programs designed to detect keystrokes cannot spy on the password. Moreover, they keypad is designed to look different for each user, and will only display a selected number of characters, so if the keypad looks unfamiliar, or does not have all of the digits in the user's password, they will know they are not at the genuine site. Tricerion also suggest using symbols for the password that are unique to a particular online service, such as a banking website. The user can only enter their password on a keypad displayed on the genuine site, meaning they cannot accidentally divulge it to a third party, eg via a phishing email.

7.5 These are examples of good practice that could be explored further. More research on novel ways to circumvent phishing scams or spyware would be of great benefit.

8. *Who should be responsible for ensuring effective protection from current and emerging threats?*

8.1 Operating system vendors are in the strongest position to build effective tools. There would be value in exploring ways that vendors could be made legally culpable when faults lead to security problems.

8.2 However, security threats to computer users are well-publicised, so there is also an onus on the users to protect themselves. They could receive assistance in this matter by making self-protection easier, in the ways described above.

9. *What is the standing of UK research in this area?*

9.1 The UK has many well respected researchers in this area and is probably second only to the USA in the field.

Governance and Regulation

10. *How effective are initiatives on IT governance in reducing security threats?*

10.1 Unless the issue of Internet Governance is resolved there is very little possibility of resolving the Personal Internet Security issue. The OII is involved with efforts to inform the new Internet Governance Forum, set up by the UN, and is supportive of security being one of the key issues that the forum should pursue.

10.2 However, initiatives in this area are frequently effective in the area of corporate security but with home users there is much less evidence of success. It is arguable that the best way to address security is to inform and empower users and to participate in balanced and credible efforts to achieve self-governance for Internet entities.

11. *How far do improvements in governance and regulation depend on international co-operation?*

11.1 The international nature of the Internet means that threats from the Internet are an international problem. Hence Internet governance is not an issue for an individual government, it is a global issue that concerns every individual globally and one country cannot legislate for all.

11.2 It is important to be aware that some governments have the objective to control and restrict the individual freedom of expression on the Internet, and wish to impose censorship rules. All governments should sign and adhere to an Internet user's "bill of rights". It is often the case that some countries with the strong views actually have low Internet penetration and usage. Hence a "one country equals one vote" rule should not always apply.

11.3 It is important that in Internet governance there is co-operation between various branches of government and law enforcement in and between countries. Civil society should be fully involved and take part in the process, which should be fully transparent. User and business associations (NGOs) should be represented directly in any regulatory body, not just through their national governments.

12. *Is the regulatory framework for Internet services adequate?*

12.1 The Internet has benefited hugely from the very light hand of regulation to date and those benefits almost certainly outweigh the risks. Further regulation would be likely to reduce the social and economic benefits of the Internet.

12.2 There is, however, one area in which regulation of software and services might help security, although it is likely to be very unpopular with software vendors. At present most software vendors demand, in their End User License Agreement, that the user gives up any right of recourse in the event that faulty software leads to loss or damage to the user's data. Furthermore, some vendors refuse to fix security problems in older versions of software and demand that users pay to upgrade to a more recent version in order to gain access to security fixes. There would be value in investigating the potential benefit to end users of imposing restrictions on these practices.

13. *What, if any, are the barriers to developing information security systems and standards and how can they be overcome?*

13.1 The barriers to developing information security systems are cost and inertia. New systems with better security characteristics are being developed all the time but it takes time before users upgrade and, as mentioned above, they frequently have to pay for the privilege of better security.

Crime Prevention

No comments from The Royal Academy of Engineering.

20 October 2006

Extract from memorandum by SecureTrading

Introduction

1. SecureTrading—a wholly-owned subsidiary of UC Group—is a privately owned company registered in the UK which operates a payments business that specialises in the secure processing of Internet payments.

2. For any online transaction which results in the transfer of monetary value from one party to another there needs to be a mechanism to transfer that value which is secure, 100% reliable, and trusted by all parties involved, ie consumer, seller, merchant, credit card company, and bank. This requires the combination of excellent security and payments technologies, strong relationships with banking and credit card partners, the ability to operate internationally, and a trusted brand. The prize for achieving this is an income stream that grows not only from the increased numbers of merchants wishing to take payments online, but also from the growth in the numbers of transactions from each merchant, and the ultimate opportunity to process other types of payments on behalf of the parties involved using internet protocols for transmission.

Defining the Problem

What is the nature of the security threat to private individuals? What new threats and trends are emerging and how are they identified?

3. Credit card transactions using the Internet involve risks not present in face-to-face business because the card holder and the merchant are not normally together when the transaction occurs. Without safeguards in place, the lack of face-to-face communication has the potential to increase the risk of fraud and money laundering in any Internet credit card transaction by comparison to its counterpart in the physical world. Some e-commerce sectors, such as gambling, entertainment and the travel industry raise additional public interest concerns that further enhance the need for making on-line credit card transactions both secure and capable of preventing fraud and other abuses.

4. The provision of online payment services underpins the use of the Internet for commerce and creates new channels for entertainment industries. It is a market that is growing rapidly.

5. In the past, organised crime groups concentrated their efforts in areas such as drug trafficking, bank robberies and prostitution. The exponential expansion of the internet and weaknesses in personal internet security has led to organised crime turning its attention to Internet users. They employ technical expertise to propagate malicious code (viruses, trojans and worms) designed to steal personal information which can be used to defraud users and to use their identities to make unauthorised financial transactions. Consumers and businesses need to be protected against the increasingly sophisticated means that criminals use to target them.

What is the scale of the problem? How are security breaches affecting the individual user detected and recorded?

6. The precise scale of losses is not easily quantifiable. Up to now, the banks and credit card companies have accepted liability for these losses; accurate reporting figures for these losses and the consequential losses incurred by victims and the financial institutions are hard to find. According to a recent APACS report, published in April 2006, in 2005 the total losses from online banking fraud reached £23.2 million—an increase of 90% of the previous year's total of £12.2 million. However, this fraud is growing from a very small base, which can make losses appear to grow rapidly: Online banking fraud losses (£23.2 million) are relatively small when compared with plastic card fraud losses (£439.4 million).

7. The advent of Chip & PIN has diverted criminals' attention to the Internet and so we expect losses through "card not present fraud" to escalate in line with the growth in online transactions.

8. There is no national co-ordination of e-crime reporting and no statistics which are reliable. Consequently, it is impossible to measure accurately relevant data in this area. Again, most consumers who are subjected to losses over the Internet are likely to report the loss to the merchant with whom they are transacting or their bank or credit card company.

How well do users understand the nature of the threat?

9. Information of this nature is difficult to accurately portray and we are not aware of any extensive research into whether individual users are specifically aware of phishing, pharming, identity theft and viruses as distinct threats and the respective dangers posed by each. Whilst increasing media attention on the issue of internet crime has certainly raised awareness of these dangers, Get Safe Online research quoted below suggests that a significant number of users are simply conscious of internet usage being synonymous with an increased vulnerability to internet crime and as such have been put off using it altogether.

Tackling the Problem

What can and should be done to provide greater computer security to private individuals? What, if any, are the potential concerns and trade-offs?

10. This requires a combined effort across a number of fronts:

- Perimeter protection is in the hands of ISPs, telcos and network infrastructure providers—such as CISCO. More could be done to clean-up malicious code and to prevent it being propagated down-stream to businesses and users.
- Businesses who provide products and services to support Internet users can clearly do more to provide hardware, software and infrastructure improvements to mitigate the threats and risks that are ever-evolving.
- Financial institutions could do more to offer better levels of protection to their customers—both business and consumer.
- Consumers too must take responsibility for their own protection.

11. This all comes at a cost—but arguably, a price which over time, will be less expensive than continuing to accept growing losses and the harm that results from them.

What is the level of public awareness of the threat to computer security and how effective are current initiatives in changing attitudes and raising that awareness?

12. SecureTrading is a key partner in the Get Safe Online initative, led by Government and supported by industry to raise safety and security for Internet users. The UK's increased use of online services has led to a greater exposure to internet criminals.

13. Since the instigation of the Get Safe Online initative, awareness of online crime has increased. In contrast to 2005, research this year shows that 21% of people now feel most at risk from Internet crime; only bank card fraud rates more highly and people are now significantly more afraid of internet crime than "physical" crimes such as burglary, being mugged and car theft (16, 11 and 8% respectively).

14. As a consequence of an increased awareness of the dangers of internet crime, the Get Safe Online research found that fear of falling victim to it is preventing some customers from transacting online (24%), shopping online (18%), or in some cases, whilst 17% has been put off using the internet all together, as a result of concerns about online crime.

15. Clearly a balance has to be struck between encouraging people to use the internet, while making sure they are aware of the risks in order to protect them.

What factors may prevent private individuals from following appropriate security practices?

16. Many Internet consumers may take the view that:

- little or no threat exists—that it "can't happen to me";
- someone else will pick-up the cost of any fraud that occurs;
- they haven't the time, inclination or knowledge to deal with the issues;
- it's too difficult to manage computer systems to provide optimum levels of security; and
- there is so much information out there, they don't know where to start—so they do not start at all.

17. Research from Get Safe Online suggests that, although people have become increasingly aware in the past 12 months about staying safe online, a significant knowledge gap still exists:

— 72% of respondents said they could use further information about online safety, compared to 78% of respondents last year; and
— 40% are still uncertain as to where to go for this advice, compared to 48% last year.

18. Progress in this field has been mixed:
— 83% of internet users have virus protection (compared to 80% last year);
— 78% have a firewall (75% last year);
— but, one fifth of respondents hadn't updated their virus protection in the last month; and
— 23% had opened an e-mail attachment from an unknown source.

19. Of greater concern is the fact that many people are also unwittingly increasingly their vulnerability to internet hackers, by not taking sufficient care to create secure passwords:
— 51% of respondents use the same password for more than one website; and
— 17% use personal information about themselves in passwords.

20. For those respondents who had failed to adopt basic security measures:
— 14% professed a lack of knowledge about the safety measures necessary to take;
— 12% expressed concerns about the cost of security systems; and
— 11% complained of a general lack of time to install them.

21. A large majority of the population still believe that it is the responsibility of others to protect individual users when it comes to online safety, although compared to only 15% in 2005, 24% of this year's survey respondents felt they should be primarily responsible for their own online security. However, 41% suggested big online organisations should insure their users against fraud, and nearly one in the ten pitting responsibility for online security at the door of HM Government.

Who should be responsible for ensuring effective protection from current and emerging threats?

22. We all have a role to play here—Government, business, vendors in the Internet market and consumers. As stated earlier, a concerted effort is required to ensure that criminality does not succeed in subverting a very rich medium which can bring huge benefits to society.

23. This is, by its very nature, a global issue, but it lacks the political support and motivation to take appropriate measures internationally to thwart those who use this new channel as a means to further criminal aims.

What is the standing of UK research in this area?

24. Poor. There is no authoritative research or study which details the key issues and which measures threats and risks, alongside the growth of on-line criminality. Neither is there any impartial, independent and authoritative advice which offers businesses and users appropriate help on what steps they can take to mitigate the threats and risks that exist.

Governance and Regulation

Is the regulatory framework for Internet services adequate?

25. Telcos and Tier 1 ISPs currently operate under a charter which provides them with "innocent carrier status". This in essence means that they take no responsibility for the data that flows through their networks. It might be time to examine whether this should change—at least in relation to the prevention of propagation of mailicious code. This is not a suggestion about regulating or interfering with "content".

What, if any, are the barriers to developing information security systems and standards and how can they be overcome?

26. Many standards exist in businesses that provide very adequate information security protection and bodies exist which do nothing other than concentrate on these issues. The Information Security Forum[33] is one such organisation.

27. To flow this learning throughout Government, businesses and to consumers requires a co-ordinated effort both nationally and internationally, as well as leadership from Government.

28. Indeed it would be extremely advantageous for business to know what the Government expects from UK Directors in relation to foreign laws and policy in this and other international financial processes.

[33] www.securityforum.org

Crime Prevention

How effective is Government crime prevention policy in this area? Are enforcement agencies adequately equipped to tackle these threats?

29. More resources need to be applied locally, nationally and internationally to cope with the growth in e-crime. Of course, it would help greatly to have accurate reporting statistics and to accurately quantify the financial losses that exist. The National Hi-Tech Crime Unit established in 2001 has now been absorbed within the Serious Organised Crime Agency (SOCA). Its e-crime division is equipped only to tackle level three criminality (national and internationally perpetrated serious organised criminality). This leaves a significant gap in the law enforcement response at a national, regional and local level and does not adequately provide a response to other level three crimes that are not considered by SOCA to warrant attention or resources.

Is the legislative framework in UK criminal law adequate to meet the challenge of cyber-crime?

30. Mostly it is. However, we need a fast and effective method of ensuring that the legislation is kept up-to-date with the evolving technical *modus operandi* employed by organised crime and other criminal elements.

20 October 2007

Memorandum by Margaret Smith

Who Am I?

I am currently an independent consultant. I have been an active technician then manager and then director for IT and e-commerce in the private sector for 36 years. I have been co-opted onto the IET IT sector panel. As part of that committee I was asked to comment on the Eurim response on Personal Internet Security. I believe very strongly that this is an issue that needs focus and resolution sooner rather than later. However the resolution must be practical, pragmatic and easily updateable as technological advances demand, my overriding concern is that the culture change we need to address will not happen and therefore we need to put measures in place that are practical, easy to use and not costly for the citizen.

My response is structured around the questions and follows the same format as the Eurim response. I believe the Eurim response to be a good response and so have only commented where I differ or have an additional view. I would be delighted to assist further in whatever ways are most helpful.

Defining the Problem

The problem as I see it is that technology in the guise of the Internet, mobile phones and even multi channel TV affords the citizen the ability to do things that make their lives easier/quicker/more interesting, at the same time as opening up their personal data to people that abuse this information. However to tackle the problems properly each problem needs defining correctly and fully. An action plan then needs to be created to solve these problems in order of priority. The action plans must be cost effective and not impact the citizen's ease of use too much. Many parts of society have an interest in being part of the debate but often each party looks at it from their own particular discipline. By defining the totality of each problem the correct disciplines can be pulled together. Not enough use is made of companies who specialise in protection.

New ways of storing and accessing data exacerbates the problem. For instance is the Committee looking at the position that Google is taking? For example would every citizen be aware that by using Google searches at a later date Google can publish your personal info on their search lists (unless you are knowledgeable and protect yourself).

The Government itself must follow good practice in ensuring that its own systems are both adequately secure as well as accessible and "user-friendly". They must also share widely this best practice and importantly learn from private sector best practice.

What is the nature of the security threat to private individuals? What new threats and trends are emerging and how are they identified?

The Internet is an open-access, network of networks with security and authentication constantly being added and updated. The primary funding of this security is by corporations and governments. The citizen only pays for software to protect themselves on their private PCs when they deem it to be necessary or if they have been hit. Organisations, both private and public, make sure that they set up appropriate security when opening their systems to individual use outside of the company firewall.

The Internet has changed the life of most people and has given them various capabilities at a very cheap price. Freedom. We must make sure that we don't force an overkill and reduce the benefit or put people off using the Internet. The use of skype must be included in whatever actions come out of this piece of work.

What is the scale of the problem? How are security breaches affecting the individual user detected and recorded?

The nature of e-business is that in the private sector the security teams already have information exchanges that work in real time. Could these informal exchanges be extended and used to channel information and awareness training. Most companies don't tell the police of security breach matters because "somehow" it gets to the police who "talk" to journalists. We do need to help the public recognise phishing and give them somewhere easy to report it as currently they don't.

There also needs to a central trend monitoring so that new types of attack and problem can be spotted early.

How well do users understand the nature of the threat?

There is an age thing here. There are I believe (and what I have seen) that says the young, the middle and the older users use the Internet/technology differently. These differences give rise to different actions/needs. Usability labs need to test and highlight the differences. Maybe even teen advisors and grey advisors should be recruited. The young are instrumental in using things differently to us "oldies" and we need to work on this.

Tackling the Problem

What can and should be done to provide greater computer security to private individuals? What, if any, are the potential concerns and trade-offs?

I believe that it should be up to the ISPs to block emails from certain countries who do not police things properly in their own countries. Some countries do not force a a website to close even if it is mimicking a website in another country. An example of this was a person who launched an attack against L&G by putting up websites that purported to be official sites but were there to criticise L&G. It became increasingly difficult to close the websites as they were not registered in the UK. A person would be able to say that they wanted to receive emails from that country. WWW is global and therefore there does need to be a global debate. However sorting out problems in the UK should not wait for this debate to reach conclusion.

What is the level of public awareness of the threat to computer security and how effective are current initiatives in changing attitudes and raising that awareness?

I do not believe the citizen will protect themselves with the necessary degree of rigour. In speaking to a lot of normal users of the net they simply get frustrated and give up. Awareness is vital but we cannot depend on them protecting themselves (just as in real world crime). Automatic security driven by the ISPs is more practical and more likely to address the issue.

What factors may prevent private individuals from following appropriate security practices?

Symantec currently do a lot of this help/education already. Just get them to publish it. Make it a rule of their license to do this awareness and every other appropriate vendor as well.

The school curriculum should have this as a mandatory part but it should be built by kids for kids (ie people who know). All awareness needs to address the relevant audience. Why not get a competition for 6th formers or GCSE students to build it for the country and publicise it. Do the same for the pensioners.

What role do software and hardware design play in reducing the risk posed by security breaches? How much attention is paid to security in the design of new computer-based products?

No private sector company would go for awards. Vendors would but would the public be interested in vendors winning awards.

Who should be responsible for ensuring effective protection from current and emerging threats?

The Eurim recommendation (Safety and security has to be treated as part of the mainstream corporate social responsibility and good citizenship programmes of all those who wish their customers, citizens and taxpayers to make confident use on-line products and services) is impractical and the citizen won't do this unless it is easy, quick, cheap and non-intrusive.

What is the standing of UK research in this area?

Why do we need UK research? What about all the other tech players who are more appropriate? This is global problem/issue and we should only do research if it is relevant to the culture of the UK.

Governance and Regulation

How effective are initiatives on IT governance in reducing security threats?

I totally agree with the Eurim recommendation (all proposals for new regulatory regimes must be subjected to a full systems review and impact analysis to check how they will achieve the objectives stated and at what cost to legitimate business, given current and prospective technologies and business models) however it must be done pragmatically and not with auditors.

Crime Prevention

How effectively does the UK participate in international actions on cyber-crime?

Need to involve eBay, Google and others more involved with using the net in new and revolutionary ways.

February 2007

Memorandum by THUS

Introduction

THUS plc is a leading provider of Internet, data and telecoms services in the United Kingdom. Our Internet services are principally offered under the "Demon" brand in the UK.

Internet security is of utmost importance to THUS both in terms of the security of our own network, but also the security of our customers. It is in our own interests to not only ensure the integrity of our network and brands remain intact, but also that are customers needs are also addressed. To this end we approach the problems from a number of angles:

- We have a dedicated Network Abuse team that deals with complaints and acts proactively to address issues before they become a problem.
- We participate in various working groups and forums, such as the Internet Crime Forum, the Internet Service Provider Association working groups, as well as interacting with government and law enforcement on the issues either directly or via these groups.
- We work with industry partners to ensure that issues are addressed speedily.
- We provide information to our customers and help them resolve any issues as well as providing details of what to look out for.
- Future work includes considering a "walled garden" approach to fencing off affected customers until their networks are repaired, more online advice and developing our online offerings such as our spam filtering service.

We believe that we all have a role to play in addressing security issues online and that ISPs are only part of that solution. Software companies, legislators and Internet users all have a part to play.

Defining the Problem

What is the nature of the security threat to private individuals? What new threats and trends are emerging and how are they identified?

The main issue that we see affecting customers' security is the proliferation of compromised machines that are being used to distribute the vast majority of spam. Spotting and fixing these "zombies" account for the bulk of the work of the Network Abuse team.

Although spam in itself is an issue, these zombies are being used to spread other associated security risks, such as phishing scams and viruses as well as the capturing of personal data via keyloggers.

What is the scale of the problem? How are security breaches affecting the individual user detected and recorded?

We detect breaches in a number of ways: responding reactively to reports and complaints about our customers' compromised machines and by spotting trends in the email traffic data (ie unusual patterns with email and viruses). We also monitor spam blocklists to ensure that our network is not blocked, this helps us identify new issues (ie specifically what led to us appearing on the blocklist in the first place).

We also work with partners in industry to help their customers. Specifically a number of these partners have a "spam" button which can be used to send us reports about spam originating on our network.

Furthermore we provide information to our customers when they join our services and work with them to resolve any compromised machines. We have plans to increase the amount of information that we provide to our customers as well as other technical solutions to limit the effect compromised machines have on our network and other Internet users.

How well do users understand the nature of the threat?

In dealing with the issues highlighted above, we have come up against a number of common problems:

- Customers' machines are poorly configured, so they are running as open mail proxies (allowing anyone to send email via their mail servers).
- Customers have poor password policies.
- Customers' anti-virus and anti-spyware software is not kept up to date and monitored to ensure they are functioning properly.
- Customers don't ensure that their operating systems and software are fully patched.
- Customers have poor policies for allowing who has access to their networks, particularly when it comes to laptops (that may access other networks) and wireless networks with no or poor encryption.
- When fixes are available it can take days or sometimes weeks before they catch up with the problem.
- If we provide too much information about security issues then often customers lose interest.
- Identifying the true perpetrator of the breach is too resource intensive, so most effort is on fixing the problem rather than investigating the cause.

Tackling the Problem

What can and should be done to provide greater computer security to private individuals? What, if any, are the potential concerns and trade-offs?

The Internet industry is already taking these matters seriously. Everybody though, has a role to play: software vendors to make their security tools easier to use; PC vendors to ensure that preinstalled software is properly configured, up to date and preconfigured with suitable security software, etc.

Also everyone can play a role in educating users about the dangers and how to avoid them, be they parents, concerned consumers or businesses. But, we must also be careful here not to scare people off the Internet because they are too worried about the risks, as this could be costly for the development of the economy and cost more than the risks we're trying to protect them from.

What is the level of public awareness of the threat to computer security and how effective are current initiatives in changing attitudes and raising that awareness?

According to recent press reports[34] consumers are more concerned about Internet security issues than they are of more "conventional" crimes such as burglary. But, although many may know about the various risks, they are perhaps not knowledgeable enough to spot them when they arise or fix them.

When we work with our customers to resolve issues we often find that the problem can be resolved, but push too much information at the customer and they will often lose interest. This is more likely the case with consumers than business users.

What factors may prevent private individuals from following appropriate security practices?

Lack of understanding of the issues and how to fix them, which may in part be caused by poor usability of the tools available to help.

What role do software and hardware design play in reducing the risk posed by security breaches? How much attention is paid to security in the design of new computer-based products?

This question is probably best answered by software and hardware vendors, but it would seem that the trick is to get the balance right. Too much enforced protection and the systems become unusable and frustrating to the user and get turned off; too little and the user's lack of knowledge means they are unlikely to spot problems soon enough.

Who should be responsible for ensuring effective protection from current and emerging threats?

Although Internet Service Providers like THUS are doing a lot for their own customers and therefore the Internet community as a whole, a nationwide education and safety campaign and a central point for information to educate the user is needed (services such as http://www.itsafe.gov.uk are a good start but could probably do with more exposure).

Governance and Regulation

How far do improvements in governance and regulation depend on international co-operation?

As the Internet is a global phenomenon, regulating in the UK or indeed across Europe is unlikely to prevent the bulk of issues and they are worldwide issues.

Is the regulatory framework for Internet services adequate?

We would like to see a universal ban on spam in the UK, not just spam to consumers, but to businesses also.

Crime Prevention

How effective is Government crime prevention policy in this area? Are enforcement agencies adequately equipped to tackle these threats?

Since most, of these security issues originate outside the UK, it is difficult to see how any kind of national crime prevention policy can affect this area. This needs to be approached at a European and global level.

23 October 2006

[34] http://news.bbc.co.uk/1/hi/technology/5414696.stm

Memorandum by Eur Ing Brian C Tompsett

Preamble

1. The 2nd European Conference on E-Crime and Digital Evidence (ECCE) was held in Nottingham from 12–14 September 2006. Delegates are specialists in the forensic collection evidence of all kinds of computer and Internet related crimes, and came from all over the world and many legal jurisdictions. One of the sessions of that conference was a participatory workshop which focused on the questions asked by the Select Committee. This evidence submission has been prepared from those discussions to enable the Committee to benefit from the collective expertise available at this event.

2. The Committee's preference for short submissions was noted, and as a result the detailed and technical discussions during the workshops have been reduced to summary conclusions for submission as evidence.

Computers as a Domestic Product

3. The consensus of opinion was that one of the biggest factors is the public's ignorance of computing technology and their use of a computer as if it was a home appliance, much as other high technology devices like Hard Disk video recorders, digital television, MP3 players and so forth. This impression is exploited by computer and Internet vendors in the marketing of their products. However, when the computers and Internet services are purchased by a consumer, the view of the vendor changes to one of detachment from the security problems, and a transfer of responsibility to the consumer. Consumers are expected to understand the risk areas of computers and Internet technology in detail and select appropriate mitigations and prophylactic applications, but this is rarely a factor mentioned in the sale and marketing, other than to amplify aspects of the safety of buying the product.

4. There was a strong view that the vendors should accept more responsibility for the more technical nature of the product and the risks it engenders. An example of the kind of responsibility that can be shown by a vendor would be to ensure that the latest software patches are all installed, and that the best security protection is already installed and configured by the vendor, rather than expect the consumer to be aware that they needed to install it. Computers and software should be sold fully "Internet enabled" and not just capable.

Internet Service

5. The provision of Internet Service was an area where the public was also being exposed to unnecessary risk, and there is ample scope for a regulator to improve capability in this provision. The view of the providers that they are only providers of bandwidth and not service is part of the problem, as is the promotion of Internet bandwidth as a national strategy. With Internet bandwidth comes risk of crime, and action to mitigate against that risk needs to be included with its provision. Most commercial enterprises and institutions who use computer networking employ a number of security precautions against intrusion and criminal use of their network. They include the control of certain types of traffic and access to certain Internet services and the location of server computers. Those providing Internet bandwidth should also be providing those kind of network management services, and the regulators should be taking steps to see that the best practises of the sector prevail.

6. Those that offer services on the Internet, such as site hosting, or Internet auctions often dissociate themselves from the risks to the public that their services enable. Web pages which host software of malicious intent, such as directly attacking a reader's computer through the placing of keylogging applications without permission, or the advertising of goods fraudulently, often say they are not responsible to those that fall victim. Although they may not be fully liable for the crime that results, there is often action that they could be taking to protect the public, which has much less technical expertise than they themselves do. These suppliers should be given a greater duty of care towards the public than they currently do.

Open Systems

7. The forensic examination of computers requires information regarding their design, operation and implementation to be available to criminal investigators. Criminal investigators operate both within law enforcement and in private practice so that all courts, prosecution and defence have access to proper investigation capabilities. It was noted that there is a move towards proprietary systems with undisclosed specifications which inhibit criminal investigation. These proprietary systems are often promoted as being more secure, and the secrecy is part of that security enhancement. Security through obscurity often places the

advantage in the hands of the criminal and not enforcement, and should not be lauded. A move towards more open systems was seen as a development that could assist the development of security products and forensic analysis of criminal evidence.

Law Enforcement

8. The lack of a visible presence of law enforcement on the Internet and in the prosecution of computer based crimes was noted. Many had experienced difficulties in reporting computer and Internet based crime to the authorities, despite their greater experience and knowledge of the area. Many authorities regarded computer and Internet crime as trivial or not part of their responsibility; even when the evidence showed otherwise. What is needed is a clear route to UK authorities mandated to handle computer and Internet based crime, with relevant links to appropriate international bodies. The theft of a pound from four million discrete people by a single party is currently perceived as many trivial offences whereas the theft of a single amount of four million pounds from one party is seen as a serious crime. Both incidents should be seen as similarly serious.

Memorandum by Paul Winstone

1. Introduction and Summary

This document summarises a collection of 19 years of personal computer experience using the prevalent Microsoft and Intel/AMD platform.

In my near 20 years of working on personal computers, I have seen many changes. In 1987, the main threat to most computers was the transfer of data or copying of software between PCs on floppy discs. Virus infections were rare compared to the current epidemic and few computers were connected to the Internet.

Now we have most home users connected to the Internet, corporate e-mail and other Internet connections and a proliferation of Internet sites on many subjects.

This has lead to a number of opportunities and also threats. Here is a summary of the main threats posed by simply having an Internet connection:

- Spam—e-mail that takes time to download and is the Internet equivalent of junk mail to the home. Very difficult to stop once you start getting it.
- Phishing—e-mail often delivered as spam and usually sent at random to a list of addresses. Designed mostly to steal identities or money.
- Illegal websites—the proliferation of websites and little control on content has lead to sites supporting child pornography, drug sales, weapons and supporting terrorist groups.
- Spyware—while this can be genuinely for the support of free products it can also be intrusive, bring your PC to a halt and expose you to pornography or other unwanted adverts. Usually found from suspect website pop ups or software downloads.
- Suspect websites—sometimes from an innocent looking website but usually found on:
  - pornographic websites;
  - illegal software download sites;
  - illegal music or video download sites; and
  - "cracking" or security "hacking" sites;

  Such a site may without your knowledge be downloading software that compromises data security and your identity;
- Direct attack—attacks in the form of denial of service, destruction of data etc gaining access through:
  - direct connection to networks/computers;
  - through services such as instant messaging;
  - file sharing of software that masquerades as something desirable; and
  - sabotage by employees or visitors.

- Virus attack—this could be in several forms but mainly distributed via:
  - networking—sharing of files and resources over a corporate network;
  - e-mail—either by spam or an infected PC sending out its own mail; and
  - trojans—tricking people into downloading a program that offers something desirable.
- Abuse—children and adults can be affected in multiple ways:
  - attempts at grooming children;
  - threats and abuse by e-mail and instant messages; and
  - libellous remarks posted unaudited on a website or a person faking another's identity when posting on a website.

2. Defining the Problem

The detail in section 1 is but the tip of the iceberg. How do we define the threat to individuals? The following lists users in order of increasing risk:

- Home user without Internet connection.
- Home user with dial up Internet.
- Home user with broadband connection.
- Businesses and other organisations with fast Internet and internal network.

A home user without an Internet connection is not immune unless they never install software from questionable sources and never exchange files with another person. Their data is at risk of destruction perhaps, but the risk of data theft is insignificant.

Users without Microsoft operating systems may think they are immune but this is also not the case. The risk does tend to be a lot lower simply because Microsoft designed their operating systems to be easy to control and manipulate through user developed programs. Mac OS tends to be very popular and far more secure than Windows as is the also popular Linux and other UNIX clones. They still have risks but the greater risk is not of infection but of carrying an infection. UNIX clones do get hacked but mostly for use as a means of attacking other companies or individuals.

The problem for those connected to the Internet has changed. Since the popularisation of the Internet in 1993 by the invention of the World Wide Web, Internet use has boomed. Viruses were the only known problem when I started and then you could get away without using any form of protection.

Over the 13 years since then, we have seen spam appear and a change in focus. Viruses used to be developed for notoriety only, effectively for bragging rights. Imagine a teenager declaring "I wrote that virus that caused the New York Stock Exchange to come to a halt". Your risk then was at first your PC could be damaged beyond repair (in the case of BIOS/CMOS viruses), data destruction requiring repair of operating system or just annoyance.

The focus changed from this immature attempt to promote themselves, to graduate eventually into a money generating method. The stages can be loosely defined as follows:

1. Political hacking eg military, government, campaigns against organisations.
2. Spam becomes more than a minor inconvenience when cost to download increases substantially.
3. Viruses/trojans target dial up users to extort money by changing dial up number to a premium rate number.
4. Viruses released to exploit flaws and gain personal details from organisations.
5. Attacks start to use corporate networks and individual computers to launch attacks on websites and individuals.
6. Virus releases decrease as phishing becomes more successful at getting access to bank accounts and other websites.

Viruses are still used to create for organised crime gangs a BotNet of computers that can be used to hack into computer systems or even send out millions of spam messages which may contain phishing attempts. But the scale of this problem has reduced over the past year.

Phishing and other scam e-mails eg claiming to collect money for charities or pyramid schemes are now the biggest threat to home users. Businesses (and especially government departments) are far more pro-active in reducing this risk. Some will block their staff from accessing banking websites or anything that could lose their

staff money through phishing. But there are still companies that do not have a firewall or antivirus software to protect them.

Spam in January 2005 reached an unbelievable 93% of incoming mail traffic according to Mail-Filters.com so the scale of the problem is beyond epidemic proportions. While the average computer user will just ignore messages trying to sell them Viagra, porn or body enhancement creams or pills there are more sinister spam messages. These are the real threat but how do the spammers get our e-mail addresses? The following are the most popular:

— Retrieving addresses from news groups.
— Virus infected computers sending all "harvested" addresses to spammers.
— Software used to retrieve addresses from websites.
— Software used to retrieve addresses from website registrars.
— Selling of e-mail lists.

There is little evidence to show that users understand the threat or how to minimise the risk to themselves and to others. By leaving their computers or networks unprotected or insufficiently protected, they are putting not just themselves but anyone who interacts with them by e-mail at risk.

3. Tackling the Problem

3.1 *What can be done to provide greater security?*

Legislation to make spam illegal or specifically unsolicited e-mail illegal has been completely ineffective. Tracking down the individuals that are the biggest cause of spam will only have a slight impact. To reduce the impact of spam (which should also reduce the impact of phishing and virus spread) the only effective method is likely to be limiting e-mail.

To explain this, how long will a spammers e-mail address last once they start sending out junk? At most I would expect 3–5 days. Although they hide their e-mail addresses to the best of their ability (most of the time at least) there are usually ways of finding it. I suggest that the best method of bringing about a substantial reduction in spam is to enforce a limit on all new e-mail accounts. I suggest that the following is implemented for all new accounts for a minimum of two weeks from creation:

— A maximum of 10 e-mails to be sent per day.
— Maximum attachment size of 500Kb.
— No more than five e-mail recipients per message.
— Users able to bypass this by placing £1,000 bond with provider which is taken if mail traffic exceeds specified limits.

While virus traffic is substantially reduced compared to 2004, this is simply because of organised crime and virus writers being paid to write specific viruses to harvest passwords etc and phishing e-mails. Forcing ISPs to deny Internet access (as opposed to access to their network) unless operating systems have appropriate updates, antivirus software and firewall software may help. However this could force a move to broadband Internet for all users which would not necessarily be a bad thing anyway.

We are unlikely to ever be able to eradicate virus attacks or phishing attempts and spam as for every method we use to fight it, criminals and those time wasters we call spammers, will attempt to bypass it. All we can do is reduce the risk.

3.2 *What is the level of public awareness?*

There has been plenty of publicity by nervous banks about phishing and quite rightly so. But there are still people being affected by it. At least now banks are doing far more to make their Internet banking far more secure.

But education of the public is the only way this is ever going to be brought to an end. Effectively this needs co-operation of ISPs or we are not going to get anywhere. Perhaps by filtering all e-mail and looking for known bank names eg Halifax, HSBC or NatWest and warning users that this may be a phishing attempt we might get somewhere. Relying on the simple education of users is not going to work. It seems horrible to say it but basically people are stupid. Many of us will believe an authentic looking e-mail without question when asked to "confirm our details" without thinking "Why would the bank ask us this when they already know?"

Many are ignorant of the risks of virus attack or direct hacking of their equipment. A simple free antivirus program downloaded from free.grisoft.com was tested as far more reliable than the often expensive Norton/ Symantec antivirus products. So there is no excuse for the public to say they can't afford the software.

There is even a decent free firewall available from www.zonelabs.com. The best is claimed to be Black Ice Defender available from www.iss.net but this is not too expensive for a one off investment.

The reason for a lack of public awareness is partly an apathy or technophobic reaction. People just aren't interested in anything computer related. They just see the PC, Mac etc as a means to an end to send e-mails, video chats to relatives, write letters, banking etc. This kind of person can only be dealt with by the help of the ISP. There may be a backlash from them at the thought of more work but then this will if implemented right actually reduce their workload.

3.3 *What factors prevent sensible precautions?*

Money, user apathy and technophobic reactions are the main reasons for sensible precautions being avoided. Making such essential security software free may help but then what will that cost the government? I would suggest that denying access to the Internet unless at least a free antivirus and firewall package are installed and maybe antispyware and antispam software as well is the best policy to pursue.

3.4 *What role can software or hardware play in reducing the risk?*

Perhaps a simple "box" to provide the needed security will be the answer but how much will this cost? Software as discussed can be provided that will reduce the impact but certainly in the case of antivirus software, this will only be as effective as how often it is updated.

Perhaps bringing an end to dial up Internet connections will be the only answer, with the being allowed only as a backup to those that have a broadband connection at home? For this all to work a partnership is needed between government and Internet providers or we will just keep being over run by spam and virus attacks.

3.5 *Who should be responsible for ensuring effective protection from threats?*

The ultimate responsibility does lie with the users but how do we make sure that the protect themselves? Legislation to force the co-operation of ISPs if they don't do so voluntarily may work but it's only any good if all work together. Perhaps a licensing scheme which means that those ineffective at providing security are shut down would be the answer?

3.6 *What's the standing of UK research in this area?*

Research does not appear that easy to find when searching the Internet. Publicity is more common through sites such as www.theregister.co.uk. As an example, an article from Sept 2006[35] shows that 3.8% of 1,835 UK adults quizzed said they would still respond to an unsolicited e-mail asking them to follow a link to re-enter personal security details. This is little better than banking organisation APACS discovered two years ago. At that time 4% indicated they might respond to such an e-mail. More people than before will now check message validity with their bank before responding with 39% now compared to 28% in 2004.

Even more worrying was the news that only 46.3% of people surveyed regularly update their antivirus software and just 10% have antispam software. They complain that 35% of users write a password down by their computer but this is far more secure than recording it on a file on the computer. 62.5% of those surveyed also never change their password. The frequency of password changes may not be important. If you have a secure password that is effectively nonsense then as long as you take adequate software precautions, you should be ok. Though changing a password periodically or using different passwords for different things is still a good idea.

[35] http://www.theregister.co.uk/2006/09/25/banking_security_survey/

4. Governance and Regulation

4.1 *How effective are initiatives on IT governance in reducing security threats?*

There is little evidence to suggest any initiatives are having an effect. The apparent reduction in virus attacks is down partly to a shift in focus to fraud by using phishing attacks.

4.2 *How far do improvements in governance and regulation depend on international co-operation?*

National co-operation with ISPs would make a substantial difference and if implemented correctly by all concerned may even be all that we need. However the major spam attacks come mostly from USA, Russia and China. To tackle spam at the source, international co-operation is absolutely essential.

4.3 *Is the regulatory framework for Internet services adequate?*

In some cases there is too much regulation which is ineffective. RIP act could be an example of this. Has it been effective in reducing organised crime? Probably not if you consider that phishing attacks are the result of organise crime. There is not enough regulation to reduce the opportunities for attack and this is where we have an opportunity to be world leaders rather than followers.

4.4 *What, if any, are the barriers to developing information security systems and standards and how can the barriers be overcome?*

Multiple parties being involved and the multinational nature of the Internet are clear barriers to development of security systems. Speed of Internet access is also a factor. Someone on a dial up connection may not be able to download updates very quickly to the antivirus software or operating system but they can still be attacked.

International co-operation would be the best way to tackle spam and phishing. My idea of limiting new mail accounts should have an impact if companies throughout the world co-operate in implementing it. This requires government legislation and support as there is no hope of implementing such an idea by communication with providers especially the less scrupulous ones.

5. Crime Prevention

5.1 *How effective is Government crime prevention policy in this area? Are enforcement agencies adequately equipped to tackle these threats?*

The Government has done what it can but this is clearly not sufficient. A lack of knowledge may be part of the problem and enforcement agencies ignore the opportunities that present themselves to tackle some offenders claiming it is impossible to track them down. Whatever happened to old fashioned detective work?

I have received an e-mail previously where I was being sold child pornography, weapons and illegal drugs. When I complained to police, this was ignored saying "We have no hope of finding out where this is coming from". From reading the e-mails, I had worked out that the sender was a native English speaker and had support of their provider in Russia. This should have enabled agencies such as Interpol to track down the perpetrator of the crime.

Prevention is an important part of reducing such a problem but it can only be done by national co-operation encouraged by the Government and international co-operation perhaps through the United Nations.

The solving of the crimes is going to be much harder but a police apathy insisting that detection is not possible is caused partly by a lack of knowledge. High tech detection teams where civilians work with police officers and intelligence agencies is essential to reduce the impact of these crimes.

5.2 *Is the legislative framework in UK criminal law adequate to meet the challenge of cyber-crime?*

Yes criminal law is probably sufficient but it is no good unless there are suitably experienced investigators to deal with reports. It also needs to be backed by legislation or pressure from the government to make absolutely sure that ISPs implement recommendations to reduce the impact of spam, virus attack, denial of service and other attacks.

Perhaps this should come under the control of the Information Commissioner's office? It needs to be lead by someone and perhaps detection and reduction of impact should be dealt with by one organisation rather than splitting the skills between multiple organisations.

5.3 *How effectively does the UK participate in international actions on cyber-crime?*

We are no better than any country. The USA perhaps leads the world in attempting to cut spam but it was a spectacular failure. The European Union tried the same thing with perhaps marginal success but has failed to provide anything with "teeth".

The Internet Watch Foundation (http://www.iwf.org.uk/) is hopelessly ineffective because it does not follow up on many complaints saying it is beyond their remit. This I cannot blame on them but something further definitely needs to be done.

A national task force on such matters may be a good start and co-operation with other such organisations in other countries, taking the ideals of the IWF further would show that the UK is serious about international actions on cyber crime.

Printed in the United Kingdom by The Stationery Office Limited
8/2007 375721 19585