HOUSE OF LORDS

Science and Technology Committee

5th Report of Session 2006–07

Personal Internet Security

Volume I: Report

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
£16.50 (inc VAT in UK)

HL Paper 165–I

Science and Technology Committee

The Science and Technology Committee is appointed by the House of Lords in each session "to consider science and technology".

Current Membership

The Members of the Science and Technology Committee are:

Lord Broers (Chairman)
Lord Colwyn
Lord Haskel
Baroness Finlay of Llandaff (co-opted)
Lord Howie of Troon
Lord Patel
Lord Paul
Baroness Perry of Southwark
Baroness Platt of Writtle
Earl of Selborne
Baroness Sharp of Guildford
Lord Sutherland of Houndwood
Lord Taverne

For members and declared interests of the Sub-Committee which conducted the inquiry, see Appendix one.

Information about the Committee and Publications

Information about the Science and Technology Committee, including details of current inquiries, can be found on the internet at http://www.parliament.uk/hlscience/. Committee publications, including reports, press notices, transcripts of evidence and government responses to reports, can be found at the same address.

Committee reports are published by The Stationery Office by Order of the House.

General Information

General information about the House of Lords and its Committees, including guidance to witnesses, details of current inquiries and forthcoming meetings is on the internet at: http://www.parliament.uk/about_lords/about_lords.cfm.

Contacts for the Science and Technology Committee

All correspondence should be addressed to:
The Clerk of the Science and Technology Committee
Committee Office
House of Lords
London
SW1A 0PW

The telephone number for general enquiries is 020 7219 6075.
The Committee's email address is hlscience@parliament.uk.

CONTENTS

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

References in the text of the Report are as follows:
(Q) refers to a question in the oral evidence
(p) refers to a page of written evidence

ABSTRACT

The Internet is a powerful force for good: within 20 years it has expanded from almost nothing to a key component of critical national infrastructure and a driver of innovation and economic growth. It facilitates the spread of information, news and culture. It underpins communications and social networks across the world. A return to a world without the Internet is now hardly conceivable.

But the Internet is now increasingly the playground of criminals. Where a decade ago the public perception of the e-criminal was of a lonely hacker searching for attention, today's "bad guys" belong to organised crime groups, are highly skilful, specialised, and focused on profit. They want to stay invisible, and so far they have largely succeeded. While the incidence and cost of e-crime are known to be huge, no accurate data exist.

Underpinning the success of the Internet is the confidence of hundreds of millions of individual users across the globe. But there is a growing perception, fuelled by media reports, that the Internet is insecure and unsafe. When this is set against the rate of change and innovation, and the difficulty of keeping pace with the latest technology, the risk to public confidence is clear.

The Government have insisted in evidence to this inquiry that the responsibility for personal Internet security ultimately rests with the individual. This is no longer realistic, and compounds the perception that the Internet is a lawless "wild west". It is clear to us that many organisations with a stake in the Internet could do more to promote personal Internet security: the manufacturers of hardware and software; retailers; Internet Service Providers; businesses, such as banks, that operate online; the police and the criminal justice system.

We believe as a general principle that well-targeted incentives are more likely to yield results in such a dynamic industry than formal regulation. However, if incentives are to be effective, they may in some cases need to be backed up by the possibility of direct regulation. Also, there are some areas, such as policing, where direct Government action is needed. So Government leadership across the board is required. Our recommendations urge the Government, through a flexible mix of incentives, regulation, and direct investment, to galvanise the key stakeholders.

The threat to the Internet is clear, but it is still manageable. Now is the time to act, both domestically, and internationally, through the European Union and through international organisations and partnerships.

Personal Internet Security

CHAPTER 1: INTRODUCTION

1.1. The Internet is a global network of millions of interconnected computer networks linking hundreds of millions of machines used by over a billion people. It transfers data between these machines in such a way that the computers at each end of a connection need not be aware of each other's physical location, or the technical details of the many intervening data transmission systems.

1.2. The origins of the Internet lie in the 1970s, but it was opened to commercial traffic in 1985, began to be widely used by individuals in the early 1990s and is now so important that it is deemed to be part of the critical national infrastructure of all developed nations.

1.3. The Internet underpins a considerable amount of global economic activity, permitting huge changes in traditional business models. It has also radically changed the way in which individuals are able to access information, entertain themselves, and even the way in which they meet their partners. It has undoubtedly been, and continues to be, a powerful force for good.

1.4. It is also a complex phenomenon that continues to evolve and grow at a rapid pace. In March 2007 the total number of Internet users world-wide was put at 1.114 billion, or 16.9 percent of the world's population. Internet penetration continent by continent varies from 3.6 percent in Africa to 69.7 percent in North America. In the United Kingdom Internet penetration is 62.3 percent, among the highest in Europe, with growth from 2000–2007 put at 144.2 percent.[1] Some eastern European countries have seen growth over the same period, albeit from very low levels, of well over 1,000 percent.

1.5. The fast-changing technology underpinning this growth in Internet use is very poorly understood by the vast majority of its users. Indeed, one reason for the prodigious success of the Internet is that users can "surf the web" without having to understand the technical means by which information is accessed or communicated. The many layers of technology that lie beneath the interface seen by the user, typically a software application known as a web browser, are effectively hidden. But just as the technology is for most users invisible, so are the risks.

1.6. These risks are manifold. They threaten personal security—that is to say, they may undermine the individual's ability to control the information that they have entered into or stored on connective devices such as PCs, mobile telephones, or databases operated by commercial organisations, government agencies and others. Victims typically suffer financial loss through fraud, though in cases of identity theft they may also suffer loss of reputation, or, in extreme cases, may be accused of crimes they did not commit.

1.7. Online risks may also impact upon personal safety—by which we mean they may lead to direct physical or psychological harm to the individual. One high-profile threat is that posed to children by predatory paedophiles, who conceal their true identity whilst using the Internet to "groom" potential

---

1 Source: Internet World Stats (http://www.internetworldstats.com/stats.htm).

victims. Probably far more common is the online bullying of children by their peers, while even adults who injudiciously disclose personal information online have found that their personal physical safety has been compromised.

1.8. The title of this Report is *Personal Internet Security*—we have considered primarily issues pertaining to individual experiences of the Internet. We have not generally considered business security issues, except insofar as these affect the security of the data of individual customers. Thus we have made recommendations around the theft of personal data but not around industrial espionage. Nor have we considered matters of business continuity, risks to services, or possible failure of the critical national infrastructure as a result of the Internet ceasing to operate for an extended period. These are all important issues—but outside the scope of this Report.

1.9. We have heard many analogies in the course of our inquiry. None of these analogies is exact—the Internet is not like any other technology or industry that has ever been created before. Nevertheless, we have found analogies useful, if not in developing conclusions and recommendations, then at least in structuring our evidence and our arguments in a readily comprehensible form. The analogy that underpins the structure of this report derives from road transport. Within the road transport system, the safety or security of the individual road user is protected at several levels:

- The network—roads are designed and engineered for safety, maintained, lit, sign-posted, and so on.
- The equipment that uses the network—cars and other vehicles that use the network have safety features built into their design.
- Individual users themselves—they are taught how to drive, subjected to testing; their behaviour may be monitored; social pressures are also exerted.
- The policing of the network—there is a clearly defined legal framework for the use of the network; those who breach the law risk prosecution.

1.10. These headings have helped us to establish a clear and comprehensive analytical approach to Internet security, embracing technical security (at both network and appliance level), individual behaviour, and policing. The bulk of this report is therefore structured around these main headings. First, however, we describe the background—the history of the Internet, its major technical features, and the nature of the threat faced by individual users.

Background and acknowledgments

1.11. The membership of the sub-committee is set out in Appendix 1, and our call for evidence, published in July 2006, in Appendix 3. Those who submitted written and oral evidence are listed in Appendix 2. We would like to thank all of our witnesses, as well as those who submitted articles, briefings and other materials in the course of the inquiry.

1.12. We launched this inquiry with a seminar, held at the Institution of Engineering and Technology, in November 2006, and a note of the seminar is given in Appendix 4. We are very grateful to all participants in this event.

1.13. We would like to put on record our thanks to the Deputy Ambassador in Washington, Alan Charlton, the Consul General in San Francisco, Martin Uden, and all their staff, for their help in organising a hugely valuable visit to

the United States in March 2007. We are also grateful to a number of people who, while not appearing formally as witnesses, have been extremely generous in offering assistance and advice—in particular Linda Criddle of Look Both Ways and Ed Gibson of Microsoft.

1.14. Finally, our Specialist Adviser for this inquiry was Dr Richard Clayton, of the University of Cambridge Computer Laboratory. His expertise in computer security has been invaluable to us throughout the inquiry. However, our conclusions are ours alone.

CHAPTER 2: OVERVIEW: THE INTERNET AND PERSONAL SECURITY

The Internet: basic definitions

2.1. A computer network is group of computers connected by means of a telecommunications system, so that they can communicate with each other in order to be able to share resources or information. An internet is a set of interconnected computer networks, and the Internet (capitalised to distinguish the specific example from the generic term) is the global network of interconnected networks that transmits data by means of the "Internet Protocol" (IP)—a specific set of rules and conventions that defines how information is communicated over the many disparate networks that make up the Internet.

2.2. As illustrations (such as the widely disseminated image that appears on the front cover of this Report) make clear, the Internet is not a single network, but rather a complex network of networks. These networks are linked by virtue of a shared paradigm for communicating information known as "packet switching".

2.3. Packet switching was first developed in the 1960s for the United States Department of Defense-sponsored ARPANET, the precursor of the modern Internet. When end-users communicate in a traditional "circuit switching" system a dedicated channel is established between them that others cannot use. In a "packet switching" network, the data sent between the end points are broken down into "packets", which are then routed between the various "nodes"—that is, devices—that make up the network. The routing may change from packet to packet and, at any given time, a link between particular nodes may be shared by many packets passing between different end users. Each packet carries the address to which it is sent and it is only at that end-point that the data stream is reconstructed. The way in which information is processed within the network as generic packets means that different technologies (wireless networks, fibre-optic cables, and so on) can be used interchangeably.

2.4. Packet switching underpins the Internet Protocol, allowing a more efficient and robust use of communications networks. It has also contributed to the astonishing creativity and innovation of the online world, by allowing the separation, or "abstraction", of the functions of the various layers of the network. This was described in very clear terms in a briefing paper[2] annexed to the written evidence by LINX, the London Internet Exchange:

> "The principle of Abstraction of Network Layers states that there are different layers in a network and each one has a specific function, with clear boundaries between adjacent layers. For example, only the application layer understands the content that is being carried over the network. The networking layer is only responsible for addressing and routing, and understands neither the data that it is transporting nor the physical characteristics nor location of the underlying physical layer."

2.5. Thus the fundamental core of the network, the wires, cables, and so on, can remain relatively stable whilst new communications technologies, such as

[2] Not published as evidence.

wireless networking, can be used to supplement, without needing to replace, existing infrastructure. Above the physical and datalink layers is the network layer, which deals with the transmission of packets, via intermediate routers, to their intended destinations. At the topmost layer are the applications that run on the end-user machines, interpreting data and providing a user interface. This layering is enormously valuable in allowing innovation at all levels. In the words of Malcolm Hutty, of LINX,

> "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 … This, to our mind, has been the principle reason why the Internet has been so successful … because it allows everybody to bring along their own contributions without needing everybody else's co-operation" (Q 725).

2.6. The most striking example of such innovation was the development of the World Wide Web, by Tim Berners-Lee and his colleague Robert Cailliau at CERN, which unlocked the potential of the Internet for the general user. Their proposals for a World Wide Web, published in 1990, described in outline a system that allowed both the location of pages of information by means of Uniform Resource Locators (URLs, more correctly now known as Uniform Resource Identifiers or URIs), and the creation of links between such pages of information by means of "hypertext".

2.7. Many terms that are commonplace today, such as "web page" and "website", not to mention activities such as "browsing" or "surfing", derive from the World Wide Web. Indeed, the World Wide Web and the Internet are often confused, so that there is little distinction in popular speech between "surfing the Web" and "surfing the Internet". But in reality, the World Wide Web is a system of linked documents and files, which operates over and is accessible by means of the Internet, but is entirely distinct from the network of networks, the Internet itself. Indeed, many other forms of communication, such as Internet Relay Chat (IRC), or Voice over IP (VoIP), using different protocols, co-exist with the World Wide Web on the Internet. The fact that the World Wide Web could be introduced in the early 1990s without requiring a fundamental redesign of the Internet is the most striking demonstration of the huge potential for innovation and growth inherent in the principle of abstraction of network layers.

2.8. However, the abstraction of network layers has other consequences as well. It is sometimes said that the Internet was built with no "identity layer"—in other words, the network level is designed to operate without knowing to whom and to what you are connecting. This is a necessary corollary of the abstraction of information into packets and the abstract layering of the Internet's design. In traditional telecommunications the existence of a dedicated connection between two identified end-points allows identity to be known by every part of the system. On the Internet, however, packets are effectively anonymous; they are simply chunks of data, routed highly efficiently—though to all appearances indiscriminately—around the network of networks. The information is then reassembled at the end point, by means of applications installed on end-user machines. It is these applications, not the network, that are concerned about the identity of the source of the information.

2.9. This creates fundamental problems for end-user security, which were outlined for us by Professor Jonathan Zittrain, of the Oxford Internet Institute: "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" (Q 957).

Tracing Internet traffic

2.10. The previous section describes in general terms the structure of the Internet and the difficulty of identifying and tracing the packets of data that traverse it. This section provides more technical detail on traceability.

2.11. Every machine directly connected to the Internet is given a unique identity, a 32-bit value called its "IP address".[3] The routing systems ensure that packets are delivered to appropriate machines, by consulting the destination IP address placed into the packet by the sender. To avoid every router having to know the location of every machine, the address space is arranged in a hierarchical manner with blocks of addresses (of varying sizes from hundreds to millions) being allocated to Internet Service Providers (ISPs). The ISPs then make allocations from these blocks to their individual customers. Thus routers need only ascertain the address block and relay the packet to the appropriate ISP. Once the packet arrives at the ISP, it can use more fine-grained routing information to deliver it to the correct machine.

2.12. When a new connection is made to a computer that is offering an Internet service, it will determine where to respond by inspecting the "source address" of the incoming packet. It sends a packet back to that source, and—provided that an acceptable reply is received from that source (some random numbers are included in these "handshake packets" to prevent spoofing)—it will then open the connection and be prepared to send and/or receive real data.

2.13. If the connection turns out to be abusive—for example, it is an incoming spam email advertising fake medicines—then the source address can be traced back by determining which block of addresses it comes from, and hence which ISP allocated the address. The records at that ISP can then identify the customer to whom the IP address was issued. Since many ISPs allocate the same address to different customers at different times, the exact time of the connection will be often be needed, in order to correctly identity the customer who was using these "dynamic addresses".

2.14. This "traceability" of IP addresses therefore permits the identification of the source ISP—who may be prepared to act to prevent further abuse. It also permits the identification of the customer account, although the ISP may not be prepared to divulge this information until the necessary legal paperwork has been processed in the appropriate jurisdiction.

2.15. However, if the requirement is to identify who is ultimately responsible for the abusive act, then considerable further investigation may be required. The source may be a machine in a cyber-café, or a hotel, available for many

---

[3] Although 32-bit addresses are by far the most prevalent, some machines operate with "IPv6", a more recent version of the Internet Protocol, which uses 128-bit addresses.

people to use. The source may be a wireless connection, in an airport, a company or an individual's home that can be used by anyone within transmission range. Most commonly of all, the source will be an identifiable consumer's machine—but if it is insecurely configured or is inadvertently running a malicious program, then it may be innocently relaying traffic from elsewhere and the tracing will need to be recommenced to determine where that might be. In practice, "multi-hop" tracing is seldom attempted and even less often successful.

Security threats on the Internet today

2.16. The design of the Internet Protocol permits the mounting of "denial of service" attacks. Here, many machines running malicious programs will send packets to a single machine—which is overwhelmed by the traffic and cannot respond to legitimate connections. Since the senders are not interested in return traffic, they can fake the source addresses in their packets, making it much harder to identify the source of the attack. Alternatively in a "reflection attack", they can send packets to legitimate machines, but with the source address set to the machine to be attacked—which will then receive responses from lots of machines that are perfectly identifiable, but are merely providing valid responses to the packets they are sent.

2.17. These types of attacks are usually called "distributed denial of service" (DDoS) attacks, and there will be large numbers, normally thousands, of machines participating in them. In some cases they can threaten the integrity not of individual machines, but of Government or company networks or top level domain names (such as ".uk" or ".com"). On 7 February 2007 a DDoS attack, emanating from sources in the Asia-Pacific region, was launched on nine of the 13 "root servers" that support the domain name system. It was unsuccessful, but as we heard when visiting Verisign, which runs two of these root servers, the level of bad traffic is now peaking at 170 times the basic level of Internet traffic; by 2010 it is predicted to be 500 times the basic level. Massive over-capacity and redundancy is built into the network to allow enough headroom to accommodate such traffic. This affects critical national infrastructure rather than personal Internet security in the first instance, and we have therefore not explored this issue in detail.

2.18. A major cause of abusive traffic on the Internet, be it DDoS attacks or the sending of email spam, is the presence of malicious code, or malware, on consumer machines. It used to be considered to be important to distinguish between "worms" that spread to vulnerable machines without human intervention and "viruses" that attach themselves to other traffic, such as email. However, the distinctions have blurred considerably in recent years and we will use the generic term "malware". This malware can still arrive via email, or via direct connections from other machines—but an important new source of infection is from visiting a website and inadvertently downloading the malicious code. The website may have been specially devised to spread infection, or it may be a legitimate site that is itself insecure, the owner unaware of its unwanted new functionality.

2.19. In general terms, malware used to be created by individuals who wanted to become famous and gain the admiration of their peers. The aim was to spread as far and as fast as possible—demonstrated most famously by the "ILOVEYOU" worm of May 2000, created by a disaffected student in the Philippines. This has now changed, and the prevailing motivation for those

creating malware is to make use of infected machines in order to make money. This means that considerable effort is now put into creating malware that will spread in a low-key manner. It is designed to be hard for the infected machine's owner to detect.

2.20. Although traditional defences such as virus checkers (which determine whether a piece of code is known to be malicious) continue to be useful, they are no longer the universal shield that they once were. Jerry Martin, of Team Cymru, a network of researchers who monitor underground traffic and support Internet security, told us of the team's database of samples of malicious code, which is currently being added to at an average rate of 6,200 new samples a day. Of these samples, typically, around 28 percent were immediately detected by anti-virus software. They submitted the samples to the anti-virus companies, and a month later the average detection rate would rise to around 70 percent. In face of the flood of new malware the anti-virus companies have little option but to adopt a risk-based approach, prioritising the most dangerous malware and the most widespread.

2.21. Putting malware onto machines is often done in order to create a "botnet". The individual machines, usually called "zombies", are controlled by a "botmaster" who can command them to act as a group. Botnets are hired out by their botmasters for the purpose of hosting illegal websites, for sending email spam, and for performing DDoS attacks. These activities take place without the knowledge of the individual machine's owner—although normal traceability will enable the source of individual examples of the traffic to be identified. The total number of "zombies" is unknown, but in the course of our visit to the Center for Information Technology Research in the Interest of Society (CITRIS) at the University of California, Berkeley, we heard an estimate that the number might be of the order of five percent of all machines, or up to 20 million in total. The cost of renting a platform for spamming is around 3–7 US cents per zombie per week.

2.22. Malware can also search the hard disk of the compromised machine to locate email addresses to add to spammers' lists of where to send their email—and, more significantly for the machine's owner, it will search the hard disk for CD keys or passwords for systems such as online games. Additionally, it may install a "keylogger" which will record any passwords used for online banking, permitting the criminal to access the account and steal the money it contains.

2.23. Online banking or trading can also be compromised by so-called "phishing" attacks. The user is sent an email purporting to come from their bank or some other company with which they do business, such as eBay. It contains some sort of urgent message—an imminent account suspension, an apparently fraudulent payment that they will wish to disavow, or even a monetary reward for answering some marketing questions. Clicking on the link within the email will result in a visit to a fraudulent website that will record the user's credentials (name, account number, password, mother's maiden name and so on) so that the criminal can—once again—take over the account and transfer money.

2.24. Although phishing emails were originally written in poor English and were relatively easy to detect, they have grown in sophistication, and millions of individuals have been misled.[4] The number of phishing emails is enormous:

---

4 See http://www.gartner.com/it/page.jsp?id=498245.

in the second half of 2006 900–1,000 unique phishing messages, generating almost 8 million emails, were blocked by Symantec software alone on a typical working day[5]—though according to MessageLabs phishing still represents just 0.36 percent of total emails.[6] Bank payments association APACS recorded 1,513 unique phishing attacks directed at United Kingdom banks in September 2006, up from just 18 in January 2005 (p 29).

2.25. United States banks are by far the most targeted by phishing, with their losses estimated to be around $2 billion. Most United Kingdom banks have also been attacked, though losses have been much lower, with losses from direct online banking fraud reaching £33.5 million in 2006. However, the United Kingdom trend is firmly upwards; losses were £23.2 million in 2005 and just £12.2 million in 2004. Total losses from "card-not-present" fraud (that is, the use of stolen credit card numbers for Internet or telephone ordering of goods) in 2005 were £183.2 million (up 21 percent from 2004), of which some £117.1 million were estimated to be Internet-based (p 30). But these figures tell only part of the story, as in many cases the losses from credit card fraud are off-loaded by the banks onto merchants.

2.26. There has also been some "identity theft", where significant amounts of information about individuals is stolen and then used to impersonate them by, for example, obtaining loans in their name. However, the scale of online identity theft is unclear, with "card not present" credit card fraud also being treated as identity theft.

The scale of the problem

2.27. Figures on the scale of the problem are hard to come by. Indeed, the lack of data on identity theft is symptomatic of a lack of agreed definitions or detailed statistics on almost all aspects of Internet security. In February 2006 the Financial Services Authority estimated the cost of identity fraud to the United Kingdom economy at £1.7 billion per annum.[7] But this included over £500 million losses reported by APACS, the United Kingdom payments association, covering counterfeit cards, lost or stolen cards, card not present fraud, through to full account takeover (the latter put at just £23.8 million). It also included £215 million for missing trader VAT fraud, £395 million for money-laundering and even £63 million for the anti-fraud procedures in the UK passport office. It is impossible to deduce from these figures how much online identity theft costs the United Kingdom economy.

2.28. Still less clear is the scale of online fraud and theft. The problem here is compounded by the lack of clear definitions that might help to differentiate online fraud from "traditional" fraud. For example, Tim Wright, of the Home Office, asked how many prosecutions there had been for "e-crimes", responded, "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

---

5 Symantec *Internet Security Threat Report*, July-December 2006, http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf.

6 MessageLabs *2006 Annual Security Report*, http://www.messagelabs.com/Threat_Watch/Intelligence_Reports/2006_Annual_Security_Report#Email%20Security%20Trends%20and%20Developments%202006.

7 http://www.identitytheft.org.uk/ID%20fraud%20table.pdf.

do not know how many people have been prosecuted for e-crimes as distinct from offline crimes" (Q 25).

2.29. We understand the logic of this—fraud is fraud, child abuse is child abuse, regardless of whether offences are initiated in person or online. But in the absence of any attempt to identify crimes committed online it is simply impossible to assess the scale of the problem. Thus when we asked John Carr, Executive Secretary of the Children's Charities Coalition on Internet Safety, about the relative frequency of online abuse and abuse committed by family members, he commented that "the way the crime figures are collected does not help us with providing an objective answer … 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" (Q 251). Bill Hughes, Director General of the Serious Organised Crime Agency, argued that there "would be benefit" in identifying the e-component of conventional crimes, which "would help us to pick up on quantifying what the actual problem is" (Q 1042).

2.30. Where data are collected, they often lack context. In the United States the National Cyber Security Alliance in 2005[8] published a survey showing that 81 percent of home computers in that country lacked core protection such as up-to-date anti-virus, firewall or anti-spyware software. This survey was backed up by scans of equipment, which showed that 12 percent of users had some sort of virus infection, and 61 percent some form of spyware or adware installed on the system. But this survey was based on a sample of just 354 individuals. Nor is it possible to deduce from these figures the actual level of economic damage that these security breaches were causing to the individuals concerned.

2.31. What is abundantly clear is that the underground economy living off Internet crime is flourishing, and shares information openly online. Team Cymru have studied this phenomenon in detail, and have recently published some of their research.[9] Focusing on just one conduit of communication, Internet Relay Chat (IRC), Team Cymru show that entire IRC networks are devoted to the underground economy, with 35 to 40 particularly active servers. On a single server in a typical month in late 2005, compromised card details for sale included 31,932 Visa cards, 13,218 MasterCards, 31 American Express cards and 1,213 Discover cards (an American card company). Basic card details are on sale to fraudsters for $1 each (or $2 for United Kingdom cards); the "full info" for an account, including passwords, address details, dates of birth, mother's maiden names, and so on, can cost up to $50, allowing entire accounts to be cleared. The total value of accounts on offer on a single IRC channel over a 24-hour period was $1,599,335.80.

2.32. With money available on this scale, it is hardly surprising that those responsible for e-crime, commonly known in the IT world as the "bad guys", include major organised crime groups, typically, though not exclusively, based in eastern Europe. They are well resourced, and employ specialists to perform particular tasks, such as hacking vulnerable websites, cashing cheques, receiving goods fraudulently purchased online, and so on. In summary, the Internet now supports a mature criminal economy.

---

8 See http://www.staysafeonline.org/pdf/safety_study_2005.pdf.

9 The figures quoted are taken from *The underground economy: priceless*, by Rob Thomas and Jerry Martin, December 2006, available online at http://www.usenix.org/publications/login/2006–12/openpdfs/cymru.pdf.

2.33. We were unable to get a clear answer to questions regarding the overall cost to the United Kingdom economy, let alone the global economy, of e-crime. One of the few witnesses prepared to take a holistic approach to the question, and, in the absence of firm data, to indicate at least the sort of areas that would have to be included in a comprehensive answer, was Bruce Schneier. He drew attention, for instance, to identity fraud, with costs "in the billions", and to the "multibillion pound industry" in computer security, as well as to unknowns, such as the costs to banking, to companies whose reputation and share price are affected by security breaches, and so on. In conclusion, he could not give an answer on the cost of e-crime, just a "flavour" for what it might be (Q 527).

2.34. It is not surprising therefore that public anxiety over e-crime is growing. A survey by Get Safe Online, a partnership of Government and industry, which appeared shortly before our inquiry started, produced the startling and headline-grabbing conclusion that 21 percent of people thought e-crime was the type of crime they were most likely to encounter. It also showed that e-crime was feared more than mugging, car theft or burglary. Yet when we asked the Government about these results it was clear that they felt that this was an aberration. Geoff Smith from the Department for Trade and Industry (DTI; now replaced by the Department for Business, Enterprise and Regulatory Reform) described it as "counter-intuitive", and added that his department had been "a bit uneasy about using that as our headline message" (Q 38).

2.35. Despite the DTI's down-playing of a survey they themselves had sponsored, the lack of hard data, combined with the alarmist stories appearing day to day in the press, means that public anxiety will probably continue to grow. This raises the question, whether the Government need to do more to help establish a true picture of the scale of the problem, the risks to individuals and the cost to the economy. We believe the answer is yes. Unless the Government take action—starting with the establishment of a framework for collecting and classifying data on e-crime, and moving on to a more rigorous and co-ordinated analysis of the incidence and costs of such crime—they will never be able to develop a proportionate and effective response. Without such a response, the risk is that the enormous benefits to society that the Internet continues to offer will be wasted.

Research and data collection

2.36. The Internet is a relatively new technology, and online security is a correspondingly new academic discipline. The evidence from the Research Councils (RCUK) claimed that "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." RCUK also provided a helpful annex of major IT research projects funded by the Engineering and Physical Sciences Research Council. However, RCUK also conceded that "the UK does not specifically have a leading reputation for academic research on IT Security". It drew attention to discussions on improving collaboration between academic researchers and industry, but gave few concrete examples. The reality appears to be that there are only a few centres of IT security research in the United Kingdom—indeed, our evidence reflects the views of researchers from virtually all these centres.

2.37. Despite the quality of the research undertaken at these few centres, overall the investment in IT security research does not appear to us commensurate to the importance of the Internet to the economy or the seriousness of the problems affecting it. During our visit to the United States in March we were fortunate to be able to visit the Center for Information Technology Research in the Interest of Society (CITRIS), at Berkeley. CITRIS receives a small amount of funding from the State of California to cover operating costs, but the bulk of its funding comes from partner organisations, either within federal government or industry. It brings together technologists, social scientists and other experts in a range of multi-disciplinary, time-limited research projects. While there are several research centres within the United Kingdom working on aspects of the subject, there is a clear need for the development of a large-scale, multi-disciplinary centre such as CITRIS to act as a focus for academic and industry expertise.

2.38. It is notable that while the private sector partners supporting CITRIS include major companies in the IT and telecommunications industries, companies from manufacturing, energy and other sectors also contribute.[10] As computing becomes ever more pervasive, more and more private sector companies—for example, those providing financial services—rely on IT security, and will have an interest in sponsoring research into IT security. There is therefore an opportunity to attract a wide range of private sector partners, with diverse interests, to support a major research initiative in this area.

2.39. At the same time, there are new legal constraints affecting IT security researchers. There has been a strong tradition within the IT community of "ethical" hackers—experts, generally unpaid enthusiasts, who test out networks and security systems by attempting to "hack" them. We agree wholeheartedly with the remarks of Bruce Schneier on the importance of their work: "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" (Q 565).

2.40. However, the amendments to the Computer Misuse Act 1990, which were introduced by means of the Police and Justice Act 2006 and are expected to come into force in April 2008, introduced a new offence of making, supplying or obtaining articles likely to be used to commit computer crimes; there are also related provisions in the Fraud Act 2006. As Alan Cox told us, these are "unfortunately the same tools that you need to identify the security holes and test a security hole has been fixed and so on" (Q 327). At the time of writing, Crown Prosecution Service guidance on the application of these provisions had yet to be published—the Minister, Vernon Coaker MP, promised that they would appear "by the end of the summer" (Q 886).

2.41. More general issues, affecting IT security experts in many countries, were touched on in our discussions at CITRIS in California. Vern Paxson drew attention to restrictions on wire tapping, as well as to difficulties encountered in monitoring the incidence of malware—the only way to monitor, say, the incidence of botnets, was to set up a platform that would both receive and respond to messages from botmasters. This meant that the researchers could

---

[10] See http://www.citris-uc.org/partners/corporate.

find themselves guilty of negligence in allowing their computer to be used to propagate malware or spam to other users.

Conclusions and recommendations

2.42. **The benefits, costs and dangers of the Internet, are poorly appreciated by the general public. This is not surprising, given the lack of reliable data, for which the Government must bear some responsibility. The Government are not themselves in a position directly to gather the necessary data, but they do have a responsibility to show leadership in pulling together the data that are available, interpreting them for the public and setting them in context, balancing risks and benefits. Instead of doing this, the Government have not even agreed definitions of key concepts such as "e-crime".**

2.43. **We recommend that the Government establish a cross-departmental group, bringing in experts from industry and academia, to develop a more co-ordinated approach to data collection in future. This should include a classification scheme for recording the incidence of all forms of e-crime. Such a scheme should cover not just Internet-specific crimes, such as Distributed Denial of Service attacks, but also e-enabled crimes—that is to say, traditional crimes committed by electronic means or where there is a significant electronic aspect to their commission.**

2.44. **Research into IT security in the United Kingdom is high in quality but limited in quantity. More support for research is needed—above all, from industry. The development of one or more major multi-disciplinary research centres, following the model of CITRIS, is necessary to attract private funding and bring together experts from different academic departments and industry in a more integrated, multi-disciplinary research effort. We recommend that the Research Councils take the lead in initiating discussions with Government, universities and industry with a view to the prompt establishment of an initial centre in this country.**

2.45. **Legitimate security researchers are at risk of being criminalised as a result of the recent amendments to the Computer Misuse Act 1990. We welcome the Minister's assurance that guidance on this point will appear later in the summer, but urge the Crown Prosecution Service to publish this guidance as soon as possible, so as to avoid undermining such research in the interim.**

CHAPTER 3: THE NETWORK

The prospects for fundamental redesign of the Internet

3.1. The Internet as we know it today, the network of networks using the IP protocol, was designed almost 30 years ago, when the current uses to which it is put could not have been imagined. But just as the road network was not planned to accommodate the volumes of traffic that now use it, but grew incrementally over many years, so the networks supporting the Internet have continued to grow and develop. And just as a wholesale redesign of the road network might in principle be desirable, but is in practice simply not feasible, so there are formidable barriers to a wholesale redesign of the Internet.

3.2. The problems that derive from the fundamental design of the Internet are profound. While the Internet supports astonishing innovation and commercial growth, it is almost impossible to control or monitor the traffic that uses it. This leads in turn to many of the security problems that we have explored in this inquiry. So we have had to ask the question, whether it is possible to redesign the Internet more securely? If not, are the incremental improvements that might make it more fit for purpose being taken forward by the industry, or is intervention, by Government or regulators, needed? Or do we just have to accept a certain level of insecurity as the inevitable corollary of the level of creativity and innovation, the "generativity" of the Internet and the innumerable services that rely on it?

3.3. The response of most of our witnesses was that however desirable it might be in theory to redesign the Internet from scratch, in practice, as with the road network, it was very unlikely to happen. The Internet has over a billion users, and their equipment and applications, their knowledge of how the network functions, represent a huge capital investment. As a result, the Internet will have to change by means of gradual evolution, not radical overhaul.

3.4. Professor Mark Handley summed up this point of view: "The idea of coming up with something different without getting there incrementally from where we are here is simply not going to happen." He did concede that there were two sets of circumstance in which a more radical approach might be required—either "if the current Internet fell in a large heap for some reason and we had to rebuild it from scratch … or if something came along which was radically better in terms of cheaper or could do things the current Internet cannot do" (Q 663). But both these scenarios are very unlikely.

3.5. A similar point was made by James Blessing, of the Internet Service Providers Association (ISPA). Asked whether it would be possible to introduce an "identity layer" into the Internet, he replied, "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" (Q 724).

3.6. We are also conscious that there are many layers to the Internet, and that fundamentally redesigning the core network may not be the most economically efficient way to improve security throughout the layers. Professor Ross Anderson illustrated this point by returning to the analogy with the road network: "You do not expect that the M1 itself will filter the traffic … 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" (Q 663). The same general principle—that you need to find the most efficient, lowest-cost solution to a given security problem—applies to the Internet.

3.7. This is not to say that researchers are not looking at the design of the network. Professor Handley conceded that he and others were "doing research into network architectures which are radically different". However, the purpose of such research was to provide pointers to "where we might want to go in the future". Getting there would be an incremental process. In the meantime most of the security problems being experienced were "with systems connected to the Internet and not with the Internet itself"; in the short to medium term "what we are going to have is basically a variation on the current Internet" (Q 663).

Recommendation

3.8. **We see no prospect of a fundamental redesign of the Internet in the foreseeable future. At the same time, we believe that research into alternative network architectures is vital to inform the incremental improvements to the existing network that will be necessary in the coming years. We recommend that the Research Councils continue to give such fundamental research priority.**

The "end-to-end principle" and content filtering

3.9. Even if fundamental redesign of the Internet is not feasible, it may still be the case that specific security concerns are best addressed at the network level. However, this approach would seem to run up against the "end-to-end principle". This was described by LINX, along with the abstraction of network layers, as one of the key principles upon which past and future innovation on the Internet depends. The LINX policy paper defines the principle as requiring "that the network core should simply carry traffic, and that additional services should always be delivered at the edges of the network, by end-points, not within the network core."

3.10. There can be no doubt that the "end-to-end principle" has served the Internet well, and goes a long way to explaining why the network is so flexible and powerful. However, it has become more than a practical or technological description of how the network is built. In the words of Professor Zittrain, in a paper published in 2006, and which he copied to the committee along with his written evidence, "Many cyberlaw scholars have taken up end-to-end as a battle cry for Internet freedom, invoking it to buttress arguments about the ideological impropriety of filtering Internet traffic."[11]

3.11. The most obvious application of the end-to-end principle is to the filtering of content. Here it could be argued that the purity of the principle has already been tarnished by the interventions of policy-makers. For example, the Government have required that by the end of 2007 all ISPs offering broadband connectivity in the United Kingdom should have implemented systems to block access to child abuse images and websites. Most ISPs already provide such a blocking service; this is achieved by blocking all sites

[11] Jonathan L Zittrain, "The Generative Internet", *Harvard Law Review*, 119 (2006), p 2029.

listed on the database maintained by the Internet Watch Foundation (IWF). In other words, ISPs are not required actively to screen images and filter out those which are judged to be child abuse images; they simply take a list of websites from a trusted source and bar direct access to them.

3.12. This is a far from perfect solution to the Government's objective of preventing paedophiles from accessing child abuse images online. It relies on the IWF list being wholly accurate (an impossible task, since in reality new sites are posted online every day); the blocking schemes continue to be relatively simple to evade; and the approach also fails to address other types of communication, such as "Peer-to-Peer" file sharing between paedophiles. There is also a risk, in the words of Matthew Henton of the ISPA, that it will "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 such people" (Q 763).

3.13. The threat to the end-to-end principle is clear, even though it may be justified by the need to protect the safety of children online. At present the blocking of websites listed in the IWF database has been accepted by the industry—largely because of what Matthew Henton called "the trust that ISPs have in the IWF and in the authenticity of that database and what it contains." However, the principle that ISPs should block certain types of site could potentially be extended more widely—as James Blessing commented, "In theory [you] can block anything as long as you know what you are blocking." This could include websites blocked for political reasons—which, as Mr Blessing argued, "completely destroys the end-to-end principle" (Q 764).

3.14. Still more controversial would be a requirement for ISPs not merely to block websites contained on a given database, but actively to screen and approve the content of the traffic passing over their networks. This would be immeasurably more complex technically, though in time it may become more practical—it is worth comparing, for instance, the latest versions of some anti-virus software, which have moved from recognition of samples held on a central database to a more dynamic, "behavioural" analysis, intended to pick up code that looks like malware, even if it has never been encountered before.[12]

3.15. In addition, any requirement on ISPs to screen content would also create the difficulties that are encountered by any email filtering system today—namely, the need to avoid both false positives (blocking good traffic) and false negatives (failing to block the bad). Inevitably the ISP would come across a lot of material that it did not recognise as either good or bad, and it would be unable to make an informed decision either way. As Malcolm Hutty told us, "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" (Q 764). In such circumstances the Internet could become unusable.

3.16. It should be emphasised that such developments are not currently envisaged in the United Kingdom, or in most other countries. Indeed, the regulation of content provided across electronic networks is specifically excluded from the remit of the regulator, Ofcom, by virtue of section 32 of the Communications

---

[12] For instance SONAR (Symantec Online Network for Advanced Response).

Act. This makes the Government's insistence that consumer ISPs block sites listed on the IWF database all the more striking, in that it marks an intervention in an area specifically excluded from the remit of the industry regulator by Parliament.

3.17. The public and political pressure to protect children online continues to grow as Internet use grows, and Ofcom too has now demonstrated its interest in content, developing in partnership with the Home Office a British Standards Institute (BSI) kite mark for Internet content control software. This development of this standard was announced by the Home Secretary in December 2006, and the first kite marks will be issued in 2007.

3.18. Clearly the development of a kite mark to help parents identify effective and easy-to-use content control software that they can then install on their end-user machines, is very different from the regulation of content delivered across electronic networks. However, it does demonstrate the Internet is not a static medium—the goal-posts move all the time, and Ofcom has as a result been obliged to intervene in an area not directly envisaged in its remit. Taken in conjunction with the requirement placed upon ISPs to block child abuse images, the development of the kite mark demonstrates the growing interest across the board in content screening, which, if the emphasis moved more towards blocking within the network, rather than on the end-user machines, could ultimately lead to the erosion of the end-to-end principle.

3.19. Internationally, blocking of content for political reasons was highly publicised with the controversial deal reached between Google and the government of the People's Republic of China in January 2006, in which Google agreed to censor certain information in exchange for access to the Chinese market. Less overt filtering is also applied by search engines in other countries, including the United Kingdom. Thus, although the end-to-end principle continues to carry weight, globally, adherence to it is increasingly challenged.

Who is responsible for Internet security?

3.20. In the previous section we discussed content screening and blocking. However, this discussion masks the fact "content" is not easily definable. Common sense suggests a simple distinction between "content"—that is, text, sounds or images, the presentation through a computer or other device of information that is easily understood, and which could indeed be presented in other formats, such as books, speech, newspapers or television programmes—and what, for lack of a better word, could be described as "code"—computer programs, malware, and so on. But in the context of Internet traffic, this distinction collapses. All information that passes via the Internet is disassembled into packets of data. In the words of Professor Ian Walden, "It is all zeros and ones which go across the network, whether it is a virus, a child abuse image or a political statement" (Q 391).

3.21. This has profound implications for personal Internet security. It means that the end-to-end principle, if it is to be fully observed, requires that security measures, like content filtering, should always be executed at the edges of the network, at end-points. We have already quoted Malcolm Hutty's assessment of the risks inherent in requiring ISPs to screen content. Similar risks, but arguably still more fundamental, would apply to any requirement that ISPs screen for security risks. If ISPs, to protect themselves against possible legal liability, block unknown code, this would, in Mr Hutty's words, "prevent

people from deploying new protocols and developing new and innovative applications" (Q 764).

3.22. However, the presumption that the network should simply carry traffic, and that end-points should apply security, along with other additional services, carries, in the words of Professor Zittrain a "hidden premise". It implies that "the people at the end points can control those end points and make intelligent choices about how they will work". Neither of these assumptions, he believed, was necessarily true any longer: not only were many devices that appeared to be "end points" in fact controlled by third parties (for instance so-called "tethered devices", like mobile phones, that could be remotely re-programmed), but it was unavoidable that "people will make poor choices". He therefore argued that it was time to adopt a "more holistic approach to understand the regulatory possibilities within the collective network" (Q 979).

3.23. Moreover, we heard over and over again in the course of our inquiry that the criminals attacking the Internet are becoming increasingly organised and specialised. The image of the attention-seeking hacker using email to launch destructive worms is out of date. Today's "bad guys" are financially motivated, and have the resources and the skills to exploit any weaknesses in the network that offer them openings. For such people the principle of "abstraction of network layers" cuts no ice. As Doug Cavit, Chief Security Strategist of Microsoft, told us in Redmond, attacks are now moving both up and down through the layers—exploiting on the one hand vulnerabilities in the application layer, and on the other working down through the operating systems, to drivers, and into the chips and other hardware underpinning the whole system.[13]

3.24. We therefore asked almost all our witnesses, in one form or another, the ostensibly simple question, "who is responsible for Internet security"? We were hoping for a holistic answer, though we by no means always got one.

3.25. The Government, for example, appeared to place responsibility firmly on the individual. In the words of Geoff Smith of the DTI, "I think certainly it is to a large extent the responsibility of the individual to behave responsibly." He compared the safe behaviours that have grown up around crossing the road with the absence of an "instinct about using the Internet safely". He acknowledged that it was "partly the responsibility of Government and business … to create this culture of security," but reiterated that it was ultimately an individual responsibility: "if you give out information over the Internet to someone you do not know … and 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" (Q 62).

3.26. ISPA, the trade association representing the network operators, expressed whole-hearted support for the Government's position. They expressed their willingness to support education initiatives, but there was no doubt that they saw ultimate responsibility residing with end-users. In the words of Camille de Stempel of AOL, "ISPA agrees very strongly with the Department of Trade and Industry approach to dealing with cyber security … ISPA members are committed to working with their consumers to help address this

---

[13] See Appendix 5.

by highlighting the way in which users can minimise the threat and informing their customers how they can best protect themselves" (Q 717).

3.27. In marked contrast, the written evidence from MessageLabs, a leading manufacturer of email filtering technology, argued that security was "fundamentally a technical problem and as such will always require a technical solution, first and foremost". The problem should be addressed "in the cloud" at Internet level, through "protocol independent defensive countermeasures woven into the fabric of the Internet itself" (p 158). In oral evidence, Mark Sunner, Chief Security Analyst, repeated the argument that relying on end-users to detect and defeat security threats was unrealistic—"it has to be done by spotting the malicious code … which you can only achieve with Internet-level filtering" (Q 464).

3.28. The views of Symantec, which manufactures anti-virus and firewall software (supplied in large part to individual end-users), were subtly different again. Roy Isbell, Vice-President, agreed with Mr Sunner that there had to be "technical countermeasures to technical attacks", but argued in favour of "a multi-layered defence … to give you some defence in depth" (Q 464).

3.29. Nevertheless, the prevailing view from within the IT industry (with the exception of those representing the ISPs), was one of scepticism over the capacity of end-users to take effective measures to protect their own security. Professor Anderson told us, "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" (Q 706).

3.30. In the course of an informal discussion with industry experts hosted at Cisco Systems in California, the Internet was compared with water supply: consumers were not required to purify or boil water, when the source of contamination was within the water supply infrastructure itself. Instead suppliers were required to maintain a secure network, and treated water up to exacting standards. The end-user simply had to switch on the tap to get pure, drinkable water.

3.31. The analogy with the water network is not, of course, exact—it was immediately pointed out to us that there is no consensus on what, in the online world, is "poisonous". Nevertheless, the analogy illustrates the oddity of thrusting so much responsibility upon end-users, who may well be incapable of protecting themselves or others. Thus Bruce Schneier responded to our question on responsibility as follows: "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" (Q 529). He then proceeded to outline the many people and organisations who might reasonably take a share of responsibility for Internet security—the financial services industry, the ISPs, the software vendors (a term which we use in the sense universal within the IT industry, namely the manufacturers of software and other products, rather than the retailers), and so on.

3.32. Jerry Fishenden, of Microsoft, also outlined a "collective responsibility" for end-user security, embracing end-users themselves, the technology supplied to them, and the ways in which the laws governing Internet use were enforced through the courts (QQ 261–262). This view was echoed by Doug

Cavit, who argued that traditional defences, anti-virus software and firewalls, were no longer adequate—every layer of the system had to be defended. We support this broader interpretation of responsibility for Internet security.

3.33. It is difficult to escape the conclusion that in the highly competitive market for Internet and IT services, in which the importance and economic value or cost of security are increasingly apparent, companies have strong incentives either to promote solutions from which they stand to profit, or, as the case may be, to argue against solutions which might impose additional costs upon them. We therefore have no choice but to treat the evidence from the industry with a degree of scepticism. But this makes it all the more disappointing that the Government appear to have accepted so unquestioningly the views of one part of the industry, the network operators and ISPs, and have in the process lost sight of the technical realities of online security.

Conclusion

3.34. **The current emphasis of Government and policy-makers upon end-user responsibility for security bears little relation either to the capabilities of many individuals or to the changing nature of the technology and the risk. It is time for Government to develop a more holistic understanding of the distributed responsibility for personal Internet security. This may well require reduced adherence to the "end-to-end principle", in such a way as to reflect the reality of the mass market in Internet services.**

Network-level security

3.35. The remainder of this chapter looks at areas in which practical improvements to personal security could be achieved through action at the level of the network or of the provision of Internet services.

3.36. One such area is the security of routers and routing protocols. Routers are the main building block of the Internet—they determine where packets are to be forwarded. Criminals who gained control of major routers would be able to block traffic, or forward traffic via routes where unencrypted content could be compromised, or to spoofed websites where phishing attacks could be mounted. It is thus essential that routers are fully secure. Cisco, a major manufacturer of routers, told us that they had still not ensured that their routers shipped without fixed values for default passwords—problematic because many users failed ever to change this default. More positively, they told us that their bigger systems, such as those used at ISPs and on backbone networks, provided "two factor" authentication (see paragraph 5.17) as standard. However, although they recommended use of two factor authentication as "best practice" they were not able to compel ISPs to use it.

3.37. Routers use the Border Gateway Protocol (BGP) to swap information about routes and which ISP has been allocated particular blocks of IP addresses. However, BGP is somewhat insecure, and it is possible for a rogue ISP (or one that has been misled by a fraudulent customer) to "announce" someone else's addresses and thereby reroute traffic. There exist variants of the BGP protocol which permit the cryptographic signing of announcements, but they are not generally used. Cryptography can also be used to ensure that the friendly, human-readable names typed into web browsers are correctly translated into computer addresses, that email is not being passed to a

machine that impersonating a real server's identity, and to ensure that email travels over the network in encrypted tunnels. However, none of these systems is widely deployed, despite the potential for email to be intercepted, or websites to be spoofed.

3.38. Professor Handley argued that these network issues were a matter primarily for the technical community, not the end-user: "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" (Q 664). He believed that "the industry is moving in the right direction to address them."

3.39. However, Malcolm Hutty, of LINX, described these systems as "immature" and "experimental", before adding, "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" (Q 759). James Blessing of ISPA suggested that they were not being used because of a lack of "stable vendor support", which we understand to mean that the manufacturers of routers and other network equipment are not yet providing systems suitable for use by ISPs. He also pointed out the need for co-ordination between 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" (Q 757).

3.40. Malcolm Hutty also argued that ISPs had every incentive to invest in more secure systems: "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?" (Q 758). Nevertheless, we remain concerned that the systems that individuals rely upon to have their traffic correctly routed, to browse the correct websites, and to keep their email secure, are reliable only because no-one is currently attacking them. This seems to us to be an area where Ofcom should be looking to develop best practice, if not regulatory standards.

Internet service provision

3.41. There appears to be still greater scope for intervention at the level of the Internet Service Provider (ISP). ISPs do not typically operate the network; instead they sell access to the network to their customers, often bundled together with a range of other services, such as web-based email, telephone (conventional or VoIP), cable television and so on. They sit, in other words, near the edges of the network, providing a link between the end-user and the network.

3.42. While the broadband infrastructure is largely in place, the market for Internet services continues to grow and is highly competitive. Internet services in the United Kingdom are marketed largely on price: indeed, since 2006 the advent of "free" broadband (although in reality, as David Hendon of DTI told us, all the ISPs have done is "re-partition the costs in a certain way") has given such competition a new intensity (Q 70).

3.43. Regulation of Internet services is the responsibility of Ofcom. However, the evidence we received from Ofcom (evidence which was only provided late in the inquiry, as a result of a direct approach by the Committee), suggests that

there is very little regulation in practice. This is not entirely the fault of Ofcom—we have already noted that content is specifically excluded from Ofcom's remit by virtue of the precise definitions of what they regulate in section 32 of the Communications Act 2003. However, questions remain over Ofcom's interpretation of its residual remit.

3.44. Ofcom appears to have taken the broadest possible view of what constitutes "content" under the Act, to embrace security products as well as text or images. In the words of their written evidence: "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" (p 320). Elsewhere the memorandum echoes the Government's position that "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" (p 325).

3.45. We find Ofcom's argument entirely unconvincing. It simply describes the *status quo*—security products are at present largely run on customer equipment, and are thus outside the control of the ISPs. But this falls well short of a convincing rationale for Ofcom's conclusion that security products "are not a part of the regulated Internet access service." Why are they not a part of the regulated service? Would it not be in the interests of consumers that they should be made a part of the regulated service? Ofcom failed to provide answers to these questions.

3.46. Ofcom went still further in resisting any suggestion that its responsibility for enforcing security standards should be extended. The Society for Computers and Law (SCL) expressed concern over the enforcement of Regulation 5 of the Privacy and Electronic Communications Regulations 2003. This requires that ISPs should take "appropriate technical and organisational measures to safeguard the security" of their services. But the SCL pointed out not only that the Regulations and the parent Directive offered "no guidance or standards" on what technical measures might be appropriate, but that enforcement was the responsibility not of Ofcom but of the Information Commissioner's Office (ICO), which lacked both resources and powers to act effectively. The SCL recommended that enforcement "should be a matter for Ofcom" (p 128).

3.47. This proposal was firmly rejected in a letter from Ofcom, which stated that "Ofcom does not have a remit in the wider area of personal Internet security or indeed the necessary expertise." Ofcom insisted that the ICO was best placed to enforce the Regulations, and drew our attention to a forthcoming "letter of understanding" which would set out how the two regulators would collaborate in future (p 312).

3.48. Ofcom's interpretation of what constitutes a "regulated Internet access service" was, perhaps unsurprisingly, echoed by the ISPs themselves. Asked whether ISPs should not be obliged to offer virus scanning as part of their service, John Souter, Chief Executive Officer of LINX, asked a question in reply, "What would be the authoritative source that you would mandate as the thing to check against?" (Q 733) This is a legitimate question, and would be very pertinent if ISPs were given a statutory duty to provide a virus scanning service, but in reality companies developing and selling security

software have to answer it every day, so it is not immediately apparent why ISPs should not make use of their well-established expertise and provide users with a scanning service that is appropriate to their circumstances. Indeed, ISPs in the United States are obliged to offer a basic level of security as part of their service to customers.

3.49. In this country, on the other hand, it is left entirely to end-users, confronted as they are by bewildering and often conflicting sources of information, to take these crucial decisions. As we have noted, Ofcom treats security as an add-on, not an integral part of Internet services. As for long-term improvements in the level of security, it is assumed that the market will provide. In the words of James 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" (Q 738).

3.50. Mr Blessing's argument is plausible as far as it goes. However, it overlooks the fact that the individual choices that customers make regarding Internet services affect not just themselves but society as a whole. The Society for Computers and Law, after acknowledging the force of the free-market argument, provided a convincing rebuttal: "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 of the public, if such botnets are used for criminal purposes" (p 126).

3.51. At the opposite end of the spectrum from the ISPs, Bruce Schneier argued forcefully that ISPs should take more responsibility for security. We have already quoted his belief that the major players in the online world should take more responsibility for assisting the "average user". As far as the ISPs were concerned, his arguments were based not on abstract principle, but on practicalities:

> "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 … they should offer to my mother. I do not think they will unless the US Government says, 'You have to'" (Q 529).

3.52. This prompts a key question: is it more efficient for basic security services such as spam or virus filtering to be offered at the ISP level or at the level of the individual end-user? It is worth noting that although, according to a 2006 survey conducted by Symantec, some 90 percent of end-user machines in the United Kingdom have anti-virus software installed, this figure includes a significant number of users who never update their software, which is therefore rendered useless. John W Thompson, CEO of Symantec, told us in the course of a private discussion that he thought some 20–25 percent of computers worldwide were at risk because their users were indifferent to security. Whatever the attractions of placing responsibility upon end users, the fact is that a huge number of them are not currently exercising this responsibility. That responsibility could possibly be more efficiently exercised, and with economies of scale, by ISPs.

3.53. A second question is, whether imposing upon ISPs a responsibility to provide a basic level of security to customers would lead to the dire consequences predicted by the ISPs, in particular the stifling of innovation across the sector as a whole? We see no reason why it should, as long as a "light touch" is maintained, rather than a blanket imposition of legal liability for every security breach, however caused.

3.54. We have already drawn attention to developments in the field of content regulation—not only the insistence that ISPs block websites containing child abuse images, listed on the IWF database, but also the development of a BSI kite mark for content control software. Given that, as we have also noted, the distinction between "content" and other forms of Internet traffic is blurred, we see a strong case for introducing similar initiatives to cover personal security. Existing anti-virus and firewall technology is capable of blocking all traffic containing samples of known malicious code (using databases which companies like Symantec update daily). Such technology is not fool-proof, but it has proved its value over many years, without stifling innovation, and we can see no reason why it should not be routinely applied at ISP level.

3.55. Indeed, deployment of security software at ISP level could have one crucial benefit. Firewalls and spam filters generally work in one direction only: they are designed to prevent bad traffic reaching the end-user, but they do not always filter outgoing traffic. In particular, once the end-user machine has been infected, and is either propagating malware, or is being used as part of a botnet to send out spam, the firewall and anti-virus software will be turned off by the malware, and updating will be disabled. Moreover, the end-user himself will in all probability not be aware that his machine has a problem, and even if he is made aware of the problem (for instance, that his machine is part of a botnet), he has no incentive to fix it—he himself suffers no significant harm if his machine is sending out spam. The recipients of the spam, and the network as a whole, if the botnet is used to launch DDoS attacks, are the ones to suffer harm.

3.56. ISPs, on the other hand, are well placed to monitor and, if necessary, filter outgoing traffic from customers. If unusual amounts of email traffic are observed this could indicate that a customer's machine is being controlled by a botnet sending out spam. At the moment, although ISPs could easily disconnect infected machines from their networks, there is no incentive for them to do so. Indeed, there is a disincentive, since customers, once disconnected, are likely to call help-lines and take up the time of call-centre staff, imposing additional costs on the ISP.

3.57. This is not to say that some ISPs do not already act in this way. Matthew Henton, of the ISP Brightview, confirmed that his company will "disconnect [an infected user's] machine from the network, we will contact that user and normally they would be entirely unaware … and we will work with them to disinfect their machine and ensure that they are adequately protected against future infection" (Q 744). We applaud this approach—but are conscious that it is not universal. Doug Cavit, at Microsoft, told us that while most (though not all) ISPs isolated infected machines, they generally found it too expensive actually to contact customers to fix the problem. Nor is this service well advertised—indeed, any ISP which advertised a policy of disconnecting infected machines would risk losing rather than gaining customers.

3.58. There is thus at present a failure in incentives, both for end-users and ISPs, to tackle these problems. We do not therefore see any prospect of the market

delivering improved security across the board. At the same time, we see no reason why the sort of good practice described by Mr Henton should not, by means of regulation if necessary, be made the industry norm.

3.59. We do not advocate immediate legislation or heavy-handed intervention by the regulator. Nor do we believe that the time has yet come to abandon the end-to-end principle once and for all. But the market will need to be pushed a little if it is to deliver better security. The example of the Ofcom-sponsored kite-mark for content control software indicates one possible way forward; a similar scheme for ISPs offering security services would give consumers greater clarity on the standards on offer from suppliers, and would help achieve greater uniformity across the market-place, particularly if backed up by the promise of tougher regulatory requirements in the longer-term.

3.60. The Government did in fact indicate that they were discussing options for improving security with the Internet services industry. As Geoff Smith, of the DTI, told us: "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" (Q 70).

3.61. We welcome the fact that the Government have at least started to think about these issues. However, the discussions described by Mr Smith appear wholly open-ended; the fact that he was not even prepared to describe what was envisaged as "self-regulation", let alone "regulation", inspires little confidence. In short, the Government's actions so far have been toothless.

The "mere conduit" defence

3.62. A specific legal consequence of the approach we are recommending would be the erosion of the "mere conduit" principle, embodied in the E-Commerce Regulations of 2002[14]. This principle provides a defence for network operators against legal liability for the consequences of traffic delivered via their networks. The principle can be caricatured, in Professor Zittrain's words, as the ability of the ISP to say, "I'm just the conduit. I'm just delivering the ticking package. You can't blame me." We would not wish to see the mere conduit defence, any more than the end-to-end principle, abandoned. However, we agree with Professor Zittrain that it is now appropriate to "take a nibble out of the blanket immunity". In particular, once an ISP has detected or been notified that an end-user machine on its network is sending out spam or infected code, we believe that the ISP should be legally liable for any damage to third parties resulting from a failure immediately to isolate the affected machine (QQ 961–963).

3.63. This carries a risk. It could create a disincentive for ISPs proactively to monitor the traffic emanating from their customers—they might conclude that it was in their interests to remain ignorant of compromised machines on their network until notified by others. This would be counter-productive, and could compound existing legal constraints to do with data protection and interception of communications, which already affect security research. To guard against such an outcome, not only should ISPs be encouraged

---

[14] See Regulation 17 of the Electronic Commerce (EC Directive) Regulations 2002.

proactively to monitor outgoing traffic, but in so doing they should enjoy temporary immunity from legal liability for damage to third parties.

Voice over Internet Protocol

3.64. We raise here one further issue that emerged in out inquiry, which relates to the robustness of the network—although it is largely distinct from the other issues discussed in this chapter. This is the regulatory framework for Voice over Internet Protocol (VoIP) suppliers, and in particular their ability to offer an emergency "999" service. When we spoke to Kim Thesiger, of the Internet Telephony Service Providers' Association (ITSPA), he said that "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" (Q 782). In particular, VoIP companies have to satisfy the requirements imposed upon Publicly Available Telephone Service (PATS) providers.

3.65. Kim Thesiger expressed particular concern over the "network integrity clause" of the PATS requirements. In a "copper-based" world it was clear what "network integrity" meant. In the world of the Internet—in which, as we have noted, packets of data travel across a network of copper, fibre-optic cable, wireless signals, and so on—it is far less clear what either what constitutes "network integrity", or what control the VoIP provider can have over it. He said that the message from Ofcom was that "you must decide yourselves whether you have network integrity or not"—which, if the wrong decision was made, could expose providers to unacceptable risks in the event of network failure.

3.66. VoIP is a relatively new technology, and Ofcom's position on emergency services is still evolving. In written evidence, Ofcom drew attention to a new Code of Practice for VoIP providers, which would require them to make clear to potential customers "whether or not the service includes access to emergency services", and the level of dependence on externalities such as power supply. However, this does not address the issue of network integrity, or Kim Thesiger's point that Ofcom believed that "in order to offer 999 calls you must be PATS-compliant". In fact Ben Willis, Head of Technology Intelligence at Ofcom, told us that the regulator had recently, in effect, toughened the rules, bringing to an end a policy of forbearance on emergency services, which had been based on the principle that "it was better to have some 999 access than none at all" (Q 1030). Instead Ofcom was initiating a new round of consultation, due to be completed in summer 2007—but with no apparent commitment to clarity the position.

Recommendations

3.67. **The current assumption that end-users should be responsible for security is inefficient and unrealistic. We therefore urge the Government and Ofcom to engage with the network operators and Internet Service Providers to develop higher and more uniform standards of security within the industry. In particular we recommend the development of a BSI-approved kite mark for secure Internet services. We further recommend that this voluntary approach should be reinforced by an undertaking that in the longer term an obligation will be placed upon ISPs to provide a good standard of security as part of their regulated service.**

3.68. **We recommend that ISPs should be encouraged as part of the kite mark scheme to monitor and detect "bad" outgoing traffic from their customers.**

3.69. **We recommend that the "mere conduit" immunity should be removed once ISPs have detected or been notified of the fact that machines on their network are sending out spam or infected code. This would give third parties harmed by infected machines the opportunity to recover damages from the ISP responsible. However, in order not to discourage ISPs from monitoring outgoing traffic proactively, they should enjoy a time-limited immunity when they have themselves detected the problem.**

3.70. **The uncertainty over the regulatory framework for VoIP providers, particularly with regard to emergency services, is impeding this emerging industry. We see no benefit in obliging VoIP providers to comply with a regulatory framework shaped with copper-based telephony in mind. We recommend instead that VoIP providers be encouraged to provide a 999 service on a "best efforts" basis reflecting the reality of Internet traffic, provided that they also make clear to customers the limitations of their service and the possibility that it may not always work when it is needed.**

CHAPTER 4: APPLIANCES AND APPLICATIONS

4.1. Having a well designed and maintained road network is one thing; but if the vehicles driving on the roads are badly designed, there will be no benefit to safety. So in this chapter we turn from the Internet itself, the network and the companies who provide Internet services to end-users, to the appliances and applications, the PCs and programs, that run on that network.

Usability vs security

4.2. Despite the innovation and creativity that have characterised the development of the Internet, there is a remarkable uniformity in the products that most individuals buy and use. The introduction of IBM's "personal computer" (or PC) in 1981 led to a standardisation of processors, components and overall system design that has continued through numerous generations to the present day. In recent time, "laptops" or "notebook computers" have become popular as alternatives to "desktop" machines, but their fundamentals are essentially identical. While there is intense competition for market share between companies such as HP, Dell and a host of competitors, the technology they are selling is highly uniform. PCs are the white goods of the IT world. The only really successful rival to the PC has been the Apple Macintosh, introduced in 1984, and its successors, but they have never been dominant, and their current market share is between 10 and 15 percent.

4.3. The operating systems running on these computers are equally uniform. Microsoft's Windows operating system is almost invariably pre-loaded on PCs and laptops; Microsoft controls up to 90 percent of the operating system market. Other vendors have smaller shares. The Apple operating system has since 2000 been based on Unix; Apple's own applications run on this platform. Linux, an open-source Unix derivative, has a much smaller share of the operating system market, made up largely of more expert users.

4.4. The greatest diversity is in the applications that run on the operating systems. Here Microsoft can claim some credit: the company has generally sought to maximise the interoperability of its operating systems, and this has without doubt contributed to diversity and innovation in the development of applications. However, Microsoft has not always adopted this approach—indeed, the company's decision in 1996 to bundle Internet Explorer free of charge along with its Windows operating system destroyed the market dominance of its major rival at that time, Netscape. Moreover, many users of Microsoft operating systems do not look beyond Microsoft applications such as the Microsoft Office suite.

4.5. How has this uniformity come about, and what bearing does it have on personal security? The first point to be made, which was argued forcefully by Ross Anderson in his presentation to our introductory seminar, is that the economics of the fast-moving IT market in the 1980s and 90s, which enabled Microsoft to establish its extraordinary dominance, placed a high premium on speed and flexibility. New products had to be rushed out quickly, and in an era when the problems now associated with the Internet were almost unknown, ease of use and adaptability generally trumped security. A similar point was made to us by Laura K Ipsen and John Stewart at Cisco, who argued that Microsoft had begun by focusing on usability, later on reliability, and only now on security.

4.6. In today's market what Professor Anderson termed "network externalities" continue to play a key part. For instance, the functionality of, say, Internet Explorer, cannot be decided by Microsoft alone. Professor Anderson noted that web browsers can be set to permit JavaScript to run. JavaScript increases functionality, making it simpler to construct intricate e-commerce websites where users can purchase complex products such as airline tickets; but it also creates vulnerabilities, for example allowing users to be redirected from legitimate bank websites to phishing sites. He concluded that the Internet was riddled with—

> "Sub-optimal ways of working … 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 … It is this kind of inertia that we are up against" (Q 686).

4.7. There is thus, as Adam Laurie told us, "always a trade-off between usability and security" (Q 311). Or as Alan Cox put it, "the really secure systems have always been produced for things like military use where usability is not a factor" (Q 323). In marked contrast, as Jerry Fishenden of Microsoft told us, Windows "is part of a complex eco-system … the end user … can add on many thousands of different third party hardware devices and many thousands of different applications that people make available" (Q 269). The JavaScript example demonstrates how the existence of such third party applications can harm security.

4.8. The temptation therefore, particularly for Microsoft, given its dominant position in the market, is to improve the security of its product by locking out third party applications. This would reduce the likelihood that these applications, whose security they cannot vouch for, could have a damaging impact upon customer security. Microsoft products, which would be permitted to run, would then be purchased instead. In essence, as the evidence from Professor Anderson's Foundation for Information Policy and Research (FIPR) said, companies that have established a dominant position "may then add excessive security in an attempt to lock in their customers more tightly" (p 211).

4.9. There have already been some signs that the major companies are seeking to "lock in" of customers through security features. The recent high-profile dispute between Microsoft and the European Commission centred on security features proposed for the Vista operating system, which the Commission contended would be anti-competitive. Microsoft's appeal against some of the changes imposed by the Commission is still to be decided by the Court of First Instance, and we are not in a position to comment on the merits of the dispute. Matt Lambert, of Microsoft, insisted that the company had "always worked with other companies, including competitors, to try to make our systems as inter-operable as possible." However, as the example of Netscape (itself subject to anti-trust litigation, though not until it was too late to salvage Netscape's position in the market) demonstrates, the Windows operating system can be a powerful tool to extend Microsoft's dominance into new sectors of the market.

4.10. In contrast, Bud Tribble told us that Apple went out of its way not to ask users security questions to which they would not know the answers. Whereas

Microsoft might seek to maximise flexibility at the expense of possible insecurity, Apple would sometimes make decisions on behalf of users even if that made it more difficult to download and run third party applications. At the time we talked to Mr Tribble, Apple had decided that it would go even further with the new iPhone and make it a "closed platform", so that it would not be possible to execute any non-Apple applications. However, at the time of writing this decision was being revisited. It is argued that Apple's approach makes its machines more secure, though the precise cause and effect behind the relatively low rate of security breaches on Apple machines is unclear. There may be many other factors at play as well, not least the fact that the company's limited market share makes it a less attractive target.

4.11. We believe that it would be enormously damaging if the major software vendors were to seek to "lock in" customers and prevent the use of third party applications. The interoperability of operating systems is a key driver for innovation. Without interoperability the constant stream of new applications, many developed by the open source community, would dry up, and the Internet would ossify.

4.12. Moreover, as we have already noted, and as Alan Cox reminded us, software developers "genuinely do not know how to build a perfectly secure, useable operating system" (Q 311). Mr Cox regarded it as a research problem which would one day be solved, but until that day comes a balance will have to be struck, and end-users will inevitably have to manage a degree of insecurity. At the same time, they have the right to expect that software vendors will make every effort possible to keep this insecurity to a minimum.

Maintaining security—patching and security software

4.13. Security, as Bud Tribble told us at Apple, begins with good design. At the early stages of design, decisions will have to be made on new features, and usability, reliability and security will have to be balanced and reconciled. In all major software companies, security is now a top priority, and the latest versions of the major operating systems, Windows Vista and Apple Mac's Leopard, are generally accepted as being by far the most secure yet.

4.14. But software is not, like a car, a complete product that is finished the moment it leaves the production line. New features are rolled out all the time, flaws identified and fixes (or "patches") produced and distributed. Moreover, the criminals operating online—the "bad guys"—are well funded, typically by organised crime groups in eastern Europe, and can call on the services of expert programmers (often as a result of blackmail or coercion). They are as skilled in disassembling and analysing code as Apple or Microsoft are in developing it. The phrase we heard over and over again in our inquiry was that it was an "arms race"—never static or stable, but involving a constant testing out of the opposition, a constant raising of the stakes.

4.15. The result is that new security threats emerge at a startling rate. Symantec, for example, documented 2,526 new vulnerabilities in the second half of 2006, higher than for any previous six-month period (for comparison, the figure for the first half of 2005 was just 1,237). Furthermore, the vulnerabilities are being used by the "bad guys" far more quickly. The company's evidence notes that in late 2005 "the average vulnerability-to-exploit window was just 5.8 days" (p 149). So keeping security software up to date is crucial to maintaining good online security. If it is out of date it is

not just useless, but arguably dangerous, because it gives the user an unjustified sense of security.

4.16. In addition, operating systems and appliances must be fully patched—in other words, the security updates issued by vendors, with a view to fixing vulnerabilities, need to be regularly installed. The responsibility for installing such updates is shared between vendors and end-users. The key question for this inquiry is whether the vendors are doing enough to help end-users. In the case of Microsoft, for example, security updates are typically issued on "patch Tuesday", the second Tuesday of each month. It used to be the responsibility of users to download patches from the Microsoft website; if they failed to do so, the "bad guys" could quickly disassemble and analyse the patches, and design malware to exploit the vulnerabilities thus identified. This gave rise to the corresponding phrase "exploit Wednesday".

4.17. However, all the major vendors, including Microsoft, now give end-users the option to configure their system to down-load security updates automatically. This was described by Microsoft as their "recommended option"—though the company also provides other options, ranging from notification that patches are available to switching off automatic updates entirely (see Q 289).

4.18. This prompts a number of questions. The first is whether a "recommended option" is sufficiently robust to protect consumers. The Society for Computers and Law were clear that computers should be "supplied with the default security settings … 'turned on', with suitable guidance and warning to end-users on the risks associated with reducing the security settings" (p 126). Microsoft has itself slowly moved towards a default "on" setting for security, and, as Adam Laurie noted, "are now shipping secure by default settings" (Q 311). The open source community has moved in the same direction.

4.19. The provision of secure settings by default begs a further question, which is whether end-users adequately understand either the limitations that a high level of security places on functionality, or the implications of lowering that level from, say, "high" to "medium". As Adam Laurie continued, vendors "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" (Q 311).

4.20. More generally, security prompts are notoriously obscure, and seem to be widely ignored by users—arguably justifying Apple's approach of eliminating prompts wherever possible. Doug Cavit assured us that Microsoft was making every effort to ensure that prompts and messages were transparent, but it was clear that Microsoft's belief was that some users would sometimes find it necessary to choose potentially risky behaviour, and therefore Windows would continue to use prompts and allow end-users to make the final decision on security. The use of simple, jargon-free language is absolutely critical if Microsoft's approach is not to undermine security.

4.21. A further concern is over the state in which PCs and operating systems are actually supplied to customers. It is one thing expecting users to update operating systems and security software, but it is another matter is these systems are not up-to-date at the time of purchase. We have not received clear evidence that out-of-date software is a major problem, but can readily see that, as proposed by the FIPR, a statement accompanying the PC, stating the date up to which the software was fully patched—in effect, a "best before" date—would be of use to purchasers (p 210). At the very least, we

see no reason why operating systems should not be programmed to provide such information when run for the very first time, and why they should not automatically update themselves so as to fix any security problems when they are first connected to the Internet.

Emerging threats and solutions

4.22. We have already given a short overview of the kinds of threats facing Internet users. Attacks continue to increase in sophistication. MessageLabs, for instance, reported the emergence of "targeted Trojans", unique examples of malware targeted at particular organisations or individuals. Trojans typically masquerade as innocent programs or files, and rely on social engineering to persuade the recipient to run the file, so installing the malware "payload". This payload might be, for instance, a keylogger, which allows the author of the Trojan to capture passwords and other data. The targeted Trojan, by definition a new and unique piece of software, is particularly difficult for security software, relying as it does largely on databases of known malware, to detect.

4.23. The number of such bespoke Trojans intercepted by MessageLabs has risen from about two per week in January 2006 to one a day by January 2007. This is still a very small number, but Mark Sunner of MessageLabs noted that towards the end of 2006 "toolkits" to make such Trojans appeared online, so that criminals could "buy this capability from certain nefarious Russian websites" (Q 461). Such developments demonstrate that in the ongoing Internet arms race the "bad guys" will continue to search for and find ways to outwit the security professionals.

4.24. However, the "arms race" works both ways. New security technologies are likely to emerge in the coming years. Bud Tribble, for example, told us that Apple was conducting research into the possibility of including within the operating system a "sand-box"—a secure area in which untested programs can be executed. The Java programming language has used a sand-box to restrict individual programs for many years, but it is likely to be two or three years before a more general form of sand-box appears in mass-market operating systems designed for personal use.

Vendor liability

4.25. The preceding discussion leads onto one of the key issues raised in this inquiry—liability. At present, even if software is shipped with major flaws which give rise to security vulnerabilities, end-users who suffer loss as a result have no legal recourse against the vendors—end-user license agreements generally exclude any legal liability. As Professor Anderson put it, the Internet way of doing business is that "liability gets dumped as much as possible on the end user" (Q 646). The absence of liability, in contrast, means that there is little incentive, particularly given the high degree of uniformity across the marketplace, for vendors[15] to raise security standards. A key question therefore is whether a liability regime would create an incentive for vendors to raise standards.

---

[15] Readers are reminded that the word vendor is used in the sense universal within the IT industry, namely the manufacturers of software and other products, rather than the general English sense of retailer.

4.26. Liability is a hugely controversial issue within the IT industry. The witness to speak most forcefully in favour of a vendor liability regime was Bruce Schneier. He argued that "We are paying, as individuals, as corporations, for bad security of products"—by which payment he meant not only the cost of losing data, but the costs of additional security products such as firewalls, anti-virus software and so on, which have to be purchased because of the likely insecurity of the original product. For the vendors, he said, software insecurity was an "externality … the cost is borne by us users." Only if liability were to be placed upon vendors would they have "a bigger impetus to fix their products" (Q 537). Thus Mr Schneier had no doubt that liability was the key to creating incentives for vendors to make more secure software.

4.27. Most other witnesses, however, were opposed to the introduction of any form of liability regime. Jerry Fishenden, of Microsoft, insisted that his colleagues were "making our platform as secure as we possibly can within the complex nature of software". He drew an analogy with 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" (Q 273).

4.28. Alan Cox, a developer of open source software, focused on the possibility that a liability regime would stifle interoperability and innovation: "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" (Q 313). Bruce Schneier, on the other hand, argued "that the companies protest a little bit too much … in fact innovation is so profitable and so valuable that you will see it" (Q 530).

4.29. Legal barriers were also raised. Nicholas Bohm argued that those who suffered harm as a result of flaws in software often had no contractual relationship with the vendor that would entitle them to claim damages: "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". At the same time, he agreed that there was currently an "incentives problem", in that "the suppliers and the creators by and large do not suffer the adverse consequences to the same extent as their customers" (Q 394).

4.30. Mr Bohm's objection to a liability regime is certainly legitimate, though Bruce Schneier, while acknowledging the problem, argued that the courts would have to manage it, as they had done in other areas, where there were already "complicated case-histories of partial liability" (Q 540). Professor Anderson also concluded that "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" (Q 658). Analysing such questions of fact and reaching a judgment is what the courts do every day.

4.31. At the same time, we accept that the pace of innovation and change in the industry means that a comprehensive liability regime may not yet be feasible. New ways to use the Internet—for instance, new applications of "Peer-to-Peer" and or other types of file sharing—emerge at bewildering speed. Online fashions and behaviours change just as fast. Professor Zittrain's comment on liability was a qualified "not yet"—" 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" (Q 971). Alan Cox, while arguing against liability, did concede that there might be "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" (Q 313).

4.32. In principle, technological constraints could slow the rate of innovation, creating a more stable and mature market for software, at any time. "Moore's Law", originally an empirical observation that computing power per unit cost of silicon chips doubled approximately every 24 months, has continued to hold good for over 40 years, and has supported an astonishingly innovative industry—but there is no guarantee that this rate of progress will be sustained in future. As this Committee noted in 2002, fundamental physical constraints will at some point limit the miniaturisation potential of conventional computer chips.[16]

4.33. We are not however in a position to predict if and when the pace of change in the online world will slow. Nor can we answer a related question, namely when the industry will, in Alan Cox's words, "get better at writing secure software". But we have no doubt that at some point in the future the IT industry, like other industries, will mature: more consistent standards for software design will emerge; the rate of innovation will slow. At that point, if not before, clearer definitions of the responsibility of the industry to customers—including a comprehensive liability regime—will be needed.

4.34. In the meantime, there are many areas in which vendor liability is already appropriate. One such is where vendors are demonstrably negligent in selling products which they know to be insecure, but which they advertise as secure. In Adam Laurie's words, "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" (Q 315). As an example, he mentioned WiFi systems, where security protocols were claimed to be secure long after they had in fact been broken.

4.35. Professor Handley also argued very succinctly for imposing liability where negligence could be shown: "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 do 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" (Q 654). We agree.

4.36. Any imposition of liability upon vendors would also have to take account of the diversity of the market for software, in particular of the importance of the open source community. As open source software is both supplied free to customers, and can be analysed and tested for flaws by the entire IT community, it is both difficult and, arguably, inappropriate, to establish contractual obligations or to identify a single "vendor". Bruce Schneier drew an analogy with "Good Samaritan" laws, which, in the United States and Canada, protect those attempting to help people who are sick or injured from possible litigation. On the other hand, he saw no reason why companies

---

[16] See *Chips for Everything: Britain's Opportunities in a Key Global Market* (2nd Report, Session 2002–03), paragraphs 4.18 ff.

which took open source software, aggregated it and sold it along with support packages—he gave the example of Red Hat, which markets a version of the open source Linux operating system—should not be liable like other vendors (Q 541).

4.37. Finally, we note that moves towards establishing vendor liability would be much more effective if they were made internationally rather than by the United Kingdom alone. There is a significant cross-border market in software products, so imposing liability onto United Kingdom companies, without making foreign companies accept similar responsibilities, would risk undermining competitiveness. In addition, regulatory intervention at United Kingdom level might risk creating distortions in the internal market, so falling foul of European Union law. We were therefore encouraged by the cautious welcome given to the prospects of vendor liability by Viviane Reding, Commissioner for Information Society and Media at the European Commission:

> "We will follow the development of the industry-led initiatives in this area … 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" (Q 947).

Conclusions and recommendations

4.38. **The IT industry has not historically made security a priority. This is gradually changing—but more radical and rapid change is needed if the industry is to keep pace with the ingenuity of criminals and avoid a disastrous loss of confidence in the Internet. The major companies, particularly the software vendors, must now make the development of more secure technologies their top design priority. We urge the industry, through self-regulation and codes of best practice, to demonstrate its commitment to this principle.**

4.39. **In particular, we urge the industry to endorse the following as best practice:**

- **Increasing the provision of security advice to users when first booting up PCs or launching applications;**
- **Automatic downloading of security updates upon first connecting machines to the Internet;**
- **Ensuring that default security settings are as high as practicable, even if functionality is restricted while users are still learning about the risks they face; and**
- **An industry-wide code of practice on the use of clear and simple language in security messages.**

4.40. **However, efforts to promote best practice are hampered by the current lack of commercial incentives for the industry to make products secure: companies are all too easily able to dump risks onto**

consumers through licensing agreements, so avoiding paying the costs of insecurity. This must change.

4.41. **We therefore recommend that the Government explore, at European level, the introduction of the principle of vendor liability within the IT industry. In the short term we recommend that such liability should be imposed on vendors (that is, software and hardware manufacturers), notwithstanding end user licensing agreements, in circumstances where negligence can be demonstrated. In the longer term, as the industry matures, a comprehensive framework of vendor liability and consumer protection should be introduced.**

CHAPTER 5: USING THE INTERNET: BUSINESSES

Overview

5.1. Our focus in this inquiry has been on individual Internet users. However, once individuals have made personal information available online, whether by sending an email, or using a search engine, or opening an online bank account, they no longer have direct control over the uses to which that information is put. So, before looking at the individual, we examine the steps that businesses and other organisations processing or storing personal information in electronic form can take to improve personal Internet security.

5.2. Myriad businesses and other organisations operate online. For many the Internet is a cheap and efficient alternative to more traditional ways of doing business. The banks, for instance, make savings in staff and branches, and can afford to offer online customers better interest rates. Dedicated online traders, such as Amazon, have profoundly changed the way people shop, allowing them to search for items and compare prices more or less instantaneously. Trading sites such as eBay are still more fundamentally dependent on the Internet, relying on features such as member feedback that would not be possible in a conventional forum.

5.3. What all these businesses have in common, along with other organisations with an online presence, such as government agencies, is that they hold personal information that individual users have disclosed to them. This information may be confidential, such as account details and passwords, or it may be more directly and personally sensitive, such as health records. In either case, its loss would expose the individual to the risk of serious harm, whether financial or personal.

5.4. It would therefore seem to be incumbent on businesses operating online to protect their customers' security and safety by ensuring that the information they hold is not lost. But as the Foundation for Information Policy Research noted, "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" (p 209). There is currently no direct commercial incentive for businesses to make the security of private individuals a high priority, given that it is those individuals who typically bear the losses resulting from security breaches.

5.5. Nor is the legal regime within which businesses operate online particularly onerous. The statutory framework for protection of personal information online is found in the Data Protection Act 1998, in particular in the seventh "data protection principle" in Schedule 1 of that Act. This provides that "Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data." Enforcement of breaches of the Act is the responsibility of the Information Commissioner.

5.6. The provisions of the Data Protection Act are supplemented by the Privacy and Electronic Communications (EC Directive) Regulations 2003, which implemented the ePrivacy Directive.[17] The Regulations cover a range of

[17] 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.

issues such as calling line identification, billing and other services provided by ISPs; but for the purposes of this chapter the key areas are unsolicited communications and email "spam".

5.7. Our key questions, therefore, have been:

- What security standards are or should be observed by businesses and other organisations operating online?
- Are additional incentives needed, and if so of what kind, to raise standards?
- Does the enforcement regime provide a strong enough deterrent to those who fail to observe adequate security standards?

Security standards

5.8. The Internet offers business a huge and fast-changing market-place. One consequence is that no accurate data exist on the level of losses suffered by individuals buying and selling online. There is no uniformity of reporting, and published figures are correspondingly unreliable. There is, for example, no precise break-down of the proportion of online fraud perpetrated by means of phishing, card-not-present fraud, and so on. Colin Whittaker of APACS estimated that "phishing accounts for anywhere between 25 and 50 percent of the attacks that we see that cause losses on customer accounts" (Q 90). An estimate as imprecise as this contributes little to our understanding of what is happening.

5.9. Nor are data available on the numbers of attacks on particular banks or businesses. APACS refused to divulge any data on the numbers of attacks on banks, Mr Whittaker merely insisting that "there is no evidence that one bank is any worse or any better off than any others" (Q 96). Where there are public reporting systems, such as the FBI-run IC3 website in the United States, the vagaries of reporting still make it difficult to read much into the data. Thus we were told at the Federal Trade Commission in Washington that some 63 percent of online frauds reported to IC3 concerned online auctions[18]. It was only when we visited eBay in Silicon Valley that we were able to put this startling figure into perspective: not only are eBay and its subsidiary PayPal, in the words of Matthew Pemble, "the primary targets worldwide for phishing" (Q 108), but they also, unusually, report all frauds to the website and encourage customers to do the same.

5.10. The key point about phishing is that it works by means of social engineering—victims are persuaded to go to a fraudulent site, on which they themselves enter their account details and other personal information. No malware needs to be involved, and standard technical measures such as anti-virus software are of no use. Phishing, and the social engineering techniques employed by criminals, become more subtle all the time, and a certain proportion of individuals will always be fooled. As we were told at eBay, some victims simply do not learn from their mistakes, but will give out account details to phishers time after time.

5.11. It follows that action by the companies whose customers are targeted and whose websites are spoofed by the phishers is essential to limit the threat to e-commerce. A key measure is the rapid closing down of phishing sites. Card

---

18 This fell to 44.9 percent in 2006.

operator Visa, for instance, told us that it maintained "a dedicated resource … for investigating the phishing emails and contacting the host to get sites shut down" (p 35). This proactive approach is of course welcome, but Visa is the target of only a small proportion of phishing emails. Nor is the process of getting hosts to close down phishing sites straightforward, given that these hosts may be based anywhere in the world. As the European Information Society Group (EURIM) noted:

> "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" (p 369).

5.12. Simple administrative measures could also help. For instance, the success of phishing emails is undoubtedly boosted by the fact that banks continue to email customers. Sandra Quinn of APACS made much of the fact that "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" (Q 134). Thus to take an example at random, the page of the Lloyds TSB website offering advice on phishing states, "While we may email you from time to time, we will never send you emails asking for your Internet banking or telephone banking information either through an email or a website."[19] But while this seems clear, the fact that emails are sent at all leaves an opening for the phishers—once the possibility that banks will contact their customers by email is admitted, the social engineering skills of the "bad guys" will do the rest.

5.13. Thus the demands of marketing and those of security appear to be in direct conflict. As Philip Robinson of the Financial Services Authority asked, "if there are very large numbers of marketing material hitting your inbox … how do you determine which are real and which are not when they all often look the same?" (Q 179). In the present circumstances, we do not believe it is appropriate that banks should send unsolicited emails to customers under any circumstances.

5.14. Technical measures might also reduce the impact of phishing. A fundamental element of online transactions is that banks and merchants have to establish that the customer purporting to use their services is who he or she claims to be. At present they typically rely on what might be called "shared secrets"—information known to customer and, say, bank, but no-one else. Such secrets include passwords, or questions and answers (for instance, mother's maiden name or first primary school). All these secrets are lost if the individual can be persuaded to log onto the phishing site. Thus the system of shared secrets is, as Nicholas Bohm commented, "inherently weak" (Q 352). Its weakness has contributed, particularly since the introduction of "chip and pin", to a huge increase in the prevalence of "card not present" fraud.

5.15. One way to combat this weakness would be to introduce a system whereby websites operated by banks or other businesses offering financial services authenticated themselves to customers, rather than simply requiring customers to authenticate themselves by entering account information, card details and passwords. In the field of online shopping, Visa's new "Verified by Visa" system introduces a personalised security page (which they told us

---

[19] See http://www.lloydstsb.com/security/phishing.asp.

could not be spoofed by a phishing website) before requesting passwords (see Q 103).

5.16. Similar systems could be introduced by banks, but at present there is no uniformity across the sector. Although such a system is employed by Alliance and Leicester, Colin Whittaker's comment was that "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" (Q 115). In other words, the market will deliver.

5.17. Another solution that has been proposed is "two factor authentication". This means, as Robert Littas of Visa put it, that the bank or merchant asks for "something you have and something you know" (Q 113). In other words, not only are "shared secrets" requested, but the customer is required to demonstrate they are in possession of something (typically a token or key fob generating a random series of six-digit numbers). This offers a degree of protection, particularly against phishing—as Paul Wood of MessageLabs noted, phishing increasingly "targets banks and organisations which do not deploy … 'two factor authentication'" (Q 461).

5.18. However, two factor authentication also has its limits. The first is practical. Individuals are already overburdened by the need to remember a range of pin numbers and passwords, to such an extent that they have little choice but to write them down, so negating their very purpose. It is unlikely that they would welcome having to keep safe, and, potentially, carry around a similar number of key fobs.

5.19. There are also technical limitations. For instance, two factor authentication is still susceptible to "man in the middle" attacks, where the attacker places himself between the consumer and the bank. In addition, the emergence of new types of "Trojan horse" could undermine its usefulness. We have already described the threat posed by keyloggers, malware installed by means of Trojans, which allow criminals to monitor and record keystrokes (and even mouse movements). While two factor authentication might appear to offer a degree of protection, Paul Wood noted that the more sophisticated malware now being installed by Trojans means that "the Trojan will potentially take over your browser session after you have completed the authentication" (Q 461). In other words, the Trojan remains dormant and invisible until the victim has logged onto a (legitimate) site, for instance to check his bank account. The Trojan then allows the criminal to take control of the web browser remotely, emptying the bank account.

5.20. This is a relatively new development, albeit one witnessing what Mr Wood called "increasing activity". It is difficult to see what businesses using the Internet, such as banks, can do to counter it. Their most promising defence will be in monitoring transactions and detecting suspicious activity patterns. However, the conclusion of MessageLabs (albeit one in their own commercial interest), was that the threat could only be countered by "Internet-level filtering" (Q 464), screening out the Trojans before they reached end-users.

5.21. Notwithstanding what we have just said about Trojans, there are many simple steps that businesses using the Internet could take to improve security for their customers. Security measures have to be proportionate to the risk, and need not be over-complicated or burdensome. Furthermore, online

security must be seen within the context of general security. As Bruce Schneier commented, "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" (Q 555).

5.22. Some of the major security lapses of recent times have come about not because of the actions of online criminals, but because of simple carelessness, such as the loss of laptops. In the case of the laptop lost by Nationwide Building Society in 2006 not only were the data of 11 million customers stored on the laptop in unencrypted form, but, according to the judgment delivered by the Financial Services Authority (FSA) in February 2007, when the laptop was stolen Nationwide was unaware what data it contained and took no action for three weeks.[20]

Incentives

5.23. If businesses and financial institutions are to take the sorts of measures outlined above, if the market is to deliver, they will need to show commitment at the highest level. This leads us to the question of incentives.

5.24. Are the banks in particular sufficiently committed to the security of customers to invest in appropriate technical and other measures to protect them? The response from APACS, the trade association representing the payments industry, was discouraging. In Colin Whittaker's words, "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" (Q 120). This demonstrates extraordinary complacency. The banks make profits because they are deemed to be a safe repository for their customers' money, and inevitably that money, not the banks' own, is the target of criminals. APACS might as reasonably claim that a bank which left its doors open and dispensed with safes was not insecure because "it is their customers that are being attacked".

5.25. Incentives are needed to overcome this complacency. They are currently lacking, because the banks in particular are able to offload risks onto customers and merchants. The legal background was helpfully explained to us by Nicholas Bohm. He drew attention first to the common law principle 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". This principle has been buttressed by statute law in certain areas—for example, the Bills of Exchange Act 1882 specified that if a bank honoured a forged cheque the bank, not the customer upon whose account the cheque was drawn, would be liable (Q 352).

5.26. No such statutory codification has been applied to the world of online banking. Instead, customers must fall back on the common law principle, which Nicholas Bohm interpreted in this context as signifying that "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". Mr Bohm concluded that he "would like to see the banking system Ombudsman, the Office of Fair Trading and anybody else concerned with

---

[20] See http://www.fsa.gov.uk/pubs/final/nbs.pdf.

unfair contract terms encouraged to take a robust line" (Q 352). However, in practice this has yet to happen, and the banks do not formally accept liability for losses incurred when customers are impersonated by criminals who have stolen account details. At present the banks generally meet such losses, but they are under no obligation to do so, and as losses rise, the temptation for the banks to disclaim liability will grow.

5.27. When these points were put to the Minister, Margaret Hodge MP, her response was as follows: "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 … and it is difficult to get those parameters right. 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" (Q 864).

5.28. The Minister's comments are deeply disappointing. There is a time to rely on the invisible hand of the market, and a time to give out signals to the market that, in order to offer proper protection to consumers, it should move in a particular direction. As Bruce Schneier commented, "I do not think that 'difficult' is a reason not to try" (Q 539). In marked contrast to the position in the United Kingdom, in the United States Regulation E of the Federal Reserve Board makes banks liable for all but the first $50 of any loss incurred as a result of an unauthorised electronic fund transfer, as long as the victim notifies the bank in timely fashion. Naturally, in the case of first party fraud—when a customer disavows a transaction dishonestly—the bank can recover its money and prosecute through the courts.

5.29. However, bringing online banking into line with the rules applying to forged cheques would affect only one part of the business world. A more fundamental change, raising the profile of online security across the board, is required. A key issue is the fact that businesses are not currently required to report or publicise security breaches. The problems this creates were described in scathing terms by the FIPR:

> "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 … 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" (p 210).

5.30. The state of affairs described by the FIPR is self-defeating. For instance, in 2005–06 hackers, exploiting vulnerabilities in WiFi systems, stole the details of over 45 million payment cards from retailer TKMaxx. Although the company disclosed this massive security breach, it was, under United Kingdom law, under no obligation so to do—and no doubt many smaller but otherwise comparable breaches have gone unreported. Still less was the company obliged to take steps to inform the individual customers concerned. These customers, if informed of the breach, might have been persuaded to examine credit card and bank statements more closely, so identifying minor frauds or thefts they would otherwise have missed. Moreover, the fact of

disclosure would have given them evidence to support a *prime facie* case that they had been victims of fraud.

5.31. Thus the absence of a duty of disclosure reduces the likelihood that customers will identify, complain of and provide proof of fraud; it also, since such complaints are in turn the most likely means of prompting disclosure, leads to a vicious circle of under-reporting. As the FIPR concluded, the absence of a duty of disclosure is a key reason why "we have no really dependable statistics" regarding the incidence of online fraud. A unified, centralised reporting system for security breaches would be a key element of any legislation, which would yield huge benefits for researchers in the field.

5.32. The position in the United States stands in marked contrast to that in the United Kingdom. While there are no federal data security breach laws currently in place, state laws, introduced first in California, now apply in 35 states. When we visited the Federal Trade Commission, officials were emphatic that these laws had had a marked impact, driving numerous investigations, and leading in the Choicepoint case to the company paying $10 million in civil penalties for security breaches and $5 million in redress to customers. Both the prospect of tough penalties, and, more importantly, the prospects of public embarrassment and loss of share value, provide strong incentives to companies to prioritise data security at the highest level.

5.33. Moreover, when we visited the FBI in California, we were told of another beneficial side-effect of security breach notification laws. Whereas in the past companies would often conceal attacks on their systems so as not to damage their reputation, now, since individuals had to be informed anyway, they were far more willing to report such events to law enforcement.

5.34. In contrast, in this country, despite the principles embodied in the Data Protection Act 1998, there is no practical incentive for those holding customer data to take steps to protect it—other than in the exceptional circumstances that they are already subject to an enforcement notice from the ICO, and are thus at risk of prosecution and a £5,000 fine. Phil Jones, of the ICO, put the prevailing situation in a nutshell: "however irresponsibly the data controller behaves he does not commit an offence" (Q 366).

5.35. The laws pertaining in the United States are far from perfect—and the diversity across the states is a significant handicap. As Dr Chris Hoofnagle, a lawyer working at the CITRIS research institute, told us, different definitions of what constituted a security breach, and differences in requirements as far as demonstrating potential harm, and in reporting requirements, to some extent undermined their effectiveness, as well as the reliability of the data generated. There were also specific problems with letters that did not make it clear what steps individuals might take when their data had been stolen—indeed, in some cases notification and advice were so buried in advertising that recipients might well miss them altogether. A federal law is currently under consideration, which aims to correct these inconsistencies and deficiencies.

5.36. In addition, Bruce Schneier suggested to us that while the laws had done "a lot of good", they might also have "outlived their usefulness". The key to the value of data security breach notification, in his view, was the "public shaming" of offenders. But this relied on publicity, and the publicity was attenuated over time—"it is no longer news when someone's innovation is stolen. It happens too often". A related risk was that individuals would be

overwhelmed by breach notifications, and, lacking the information to enable them to assess the actual risks, would quickly lose interest. Nevertheless, he concluded that "I think that it should still be done, because forcing companies to go public with the information is very valuable—to researchers, to policymakers" (Q 547).

5.37. The position of the Government was lukewarm. Margaret Hodge described security breach notification as "an enticing bit of legislation", but then focused on "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 … The devil is in the detail" (Q 849).

5.38. We fully acknowledge the Minister's points—it is essential, in particular, that any obligation to disclose security breaches should set a sensible threshold in terms of the potential risk to those affected. For instance, if a laptop is lost, but the data are securely encrypted, or if the laptop was contained in the boot of a car that has driven off a bridge into a deep river, the risk of data breach may be minimal. The detail must be got right. But we believe that the United Kingdom is now ideally placed to learn from the successes and failures of the many state laws in force in the United States and get this detail right, establishing a workable and effective legislative framework.

5.39. However, we find it alarming that the Minister appeared to regard with equanimity a situation in which security breaches were so common that if companies were to be obliged to inform individuals of security breaches affecting their personal data, these individuals would respond either with bored indifference or fear. In the Foreword to his latest Annual Report, the Information Commissioner noted that "The roll call of banks, retailers, government departments, public bodies and other organisations which have admitted serious security lapses is frankly horrifying"[21]. The evidence heard in this inquiry fully bears out this description. The sheer volume of breaches must not be used as an excuse for inaction.

5.40. Mrs Hodge also drew attention to proposals emerging from the European Commission on data breach notification in the context of its new Regulatory Framework for Electronic Communications. However, as the title of this initiative implies, the Commission's proposals would place requirements solely on companies in the communications sector. They would thus omit the many businesses in banking and financial services, retailing and elsewhere, that hold confidential personal data.

5.41. The reason for this limitation appears to be bureaucratic rather than reasoned. As Achim Klabunde, of the Directorate General Information Society, said when asked why the proposals were limited to the communications sector, companies in other sectors, such as payment services, were outside his "organisational competence" (Q 910). In other words, DG Information Society has no authority to initiate proposals covering, for instance, the payment services industry. This is an inescapable fact, and inevitably means that the laws currently proposed in Brussels will

21 Information Commissioner's Office, *Annual Report 2006/07*, 10 July 2007 (HC646), p 7.

have little impact in raising the incentives for business to take the necessary steps to protect personal Internet security.

The enforcement regime

5.42. We have outlined above the role of the Information Commissioner's Office (ICO) in enforcing the statutory provisions that protect the security of personal data online. In a previous chapter we have also outlined the very limited remit of the communications industry regulator, Ofcom, with regard to Internet Service Providers.

5.43. An extra layer of regulation is provided by the Financial Services Authority (FSA), which regulates the banks and the rest of the financial services sector. Its task, set out in the Financial Services and Markets Act 2000, is to ensure that regulated companies in the sector meet the "threshold conditions" set out in Schedule 6 of the Act: in the words of the FSA, 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" (p 54).

5.44. In the field of Internet trading, the Office of Fair Trading (OFT) has a general responsibility to regulate the advertising industry. Spam, insofar as it contains misleading advertising, falls under the remit of the OFT, which also co-ordinates international action on spam through the London Action Plan. However, Mike Haley of the OFT conceded that the enforcement mechanisms were too clumsy to deal with the fast-moving and globalised market for spam:

> "Our powers are still based on the offline 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 … 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" (Q 429).

5.45. Finally, enforcement with regard to specific online scams is the responsibility of Local Trading Standards Services (LTSS). A recent OFT report acknowledges that the priority afforded to online frauds is variable; that no specific requirements relating to the Internet are contained within the National Performance Framework for LTSS; and that enforcement was generally "reactive to complaints".[22]

5.46. There are thus many divisions of responsibility and apparent overlaps. On there one hand there is, as the Minister Margaret Hodge MP told us, a "crude division of labour" between Ofcom and the ICO: "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" (Q 865). On the other hand, while the ICO has a general duty to enforce the data protection principles, including the seventh principle, that "appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data", in the vital financial

---

22 See *Internet Shopping: an OFT Market Study*, June 2007, p 101: http://www.oft.gov.uk/shared_oft/reports/consumer_protection/oft921.pdf.

services sector the FSA also has responsibility for assessing such systems and controls.

5.47. What this complicated division of responsibility between regulatory and enforcement bodies demonstrates is that the online world, as a medium that offers a constantly expanding range of uses to business, has no dedicated regulator. Instead, discrete areas of activity, such as advertising or banking, are regulated, with the divisions of responsibility between regulators being modelled on the offline world.

5.48. The only enforcement agency with a general responsibility for personal Internet security, insofar as it relates to the security of personal data, is the ICO. However, of all the regulatory authorities, the ICO's enforcement powers appear currently to be the weakest. As Phil Jones of the ICO told us, "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" (Q 365).

5.49. As a result, when the ICO found in March 2007 that 11 banks and other financial institutions had breached data protection principles by discarding personal information in waste bins, it was able only to require the companies "to sign a formal undertaking to comply with the Principles of the Data Protection Act." Further breaches "could result in prosecution"—with the maximum fine on summary conviction currently standing at just £5,000.[23] In summary, the Society for Computers and Law (SCL) concluded that the seventh data protection principle was "not rigorously enforced" (p 128).

5.50. In marked contrast, in February 2007, following the 2006 loss of a laptop containing confidential customer information (already referred to above, paragraph 5.22), the FSA fined the Nationwide Building Society £980,000 for "failing to have effective systems and controls to manage its information security risks".[24]

5.51. In late 2006 the Department for Constitutional Affairs (now the Ministry for Justice) launched a consultation on increasing the maximum penalty available to the courts for wilful misuse of personal data to six months' imprisonment.[25] The Home Office Minister, Vernon Coaker MP, confirmed that following this consultation "the Government is now looking at is a vehicle to actually look at increasing some of the penalties available for the misuse of data" (Q 876).

5.52. However, the 2006 consultation does not contain any proposals to change the cumbersome enforcement regime, including the requirement that offenders first sign undertakings to comply with the Data Protection Principles with legal action only possible if further breaches occur. Mrs Hodge told us 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" (Q 878). However, we are not

---

23 ICO press release: http://www.ico.gov.uk/upload/documents/pressreleases/2007/banks_in_unacceptable_data_protection_breach.pdf.

24 FSA press release: http://www.fsa.gov.uk/pages/Library/Communication/PR/2007/021.shtml.

25 See http://www.dca.gov.uk/consult/misuse_data/consultation0906.pdf.

aware of any measures planned which might meet the concern of the SCL, that "the resources made available to the [ICO] continue to be inadequate" (p 128).

Conclusions and Recommendations

5.53. **The steps currently being taken by many businesses trading over the Internet to protect their customer's personal information are inadequate. The refusal of the financial services sector in particular to accept responsibility for the security of personal information is disturbing, and is compounded by apparent indifference at Government level. Governments and legislators are not in position to prescribe the security precautions that should be taken; however, they do have a responsibility to ensure that the right incentives are in place to persuade businesses to take the necessary steps to act proportionately to protect personal data.**

5.54. **We therefore recommend that the Government introduce legislation, consistent with the principles enshrined in common law and, with regard to cheques, in the Bills of Exchange Act 1882, to establish the principle that banks should be held liable for losses incurred as a result of electronic fraud.**

5.55. **We further believe that a data security breach notification law would be among the most important advances that the United Kingdom could make in promoting personal Internet security. We recommend that the Government, without waiting for action at European Commission level, accept the principle of such a law, and begin consultation on its scope as a matter of urgency.**

5.56. **We recommend that a data security breach notification law should incorporate the following key elements:**

- **Workable definitions of data security breaches, covering both a threshold for the sensitivity of the data lost, and criteria for the accessibility of that data;**
- **A mandatory and uniform central reporting system;**
- **Clear rules on form and content of notification letters, which must state clearly the nature of the breach and provide advice on the steps that individuals should take to deal with it.**

5.57. **We further recommend that the Government examine as a matter of urgency the effectiveness of the Information Commissioner's Office in enforcing good standards of data protection across the business community. The Commissioner is currently handicapped in his work by lack of resources; a cumbersome "two strike" enforcement process; and inadequate penalties upon conviction. The Government have expressed readiness to address the question of penalties for one type of offence; we recommend that they reconsider the tariffs for the whole of the data protection regime, while also addressing resources and enforcement procedures as well. These should include the power to conduct random audits of the security measures in place in businesses and other organisations holding personal data.**

CHAPTER 6: USING THE INTERNET: THE INDIVIDUAL

Overview

6.1. Enormous reliance is currently being placed by Government upon education, information and training. Arguably the key question in our Call for Evidence was "What can and should be done to provide greater computer security to private individuals?" The Government's response began as follows:

> "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" (p 4).

6.2. The tone is typical of the Government's evidence to this inquiry. While there is a passing acknowledgement that Government and the industry have a "collective responsibility" in the area of personal Internet security, in practice their roles appear to be limited to making people "aware" of the risks online, and providing them with the tools "to make themselves and their families" secure.

6.3. The tenor of our Report thus far is clear: we have argued throughout for Government, regulators, the IT industry and online businesses to take more active steps to improve personal Internet security. We have recommended a range of incentives designed to ensure that those best placed and most competent to improve personal Internet security—the ISPs, software and hardware vendors, and the companies who conduct business online—are motivated to do so.

6.4. But at the same time, just as drivers are required to meet certain standards, not just for their own protection, but for the protection of other road-users, so individuals in the online world must take a measure of responsibility for their own security and that of others. We therefore begin this chapter by examining where the balance lies between individual responsibility and Government, regulatory or corporate action.

6.5. We also consider in this chapter the largely self-contained issue of online safety, the prevention of actual physical or psychological harm to individuals. This is a matter in large part of personal behaviour, though here too the IT industry and businesses operating online bear a significant responsibility.

Individual skills

6.6. There are those who argue that the astonishing rate of change and innovation which the Internet continues to witness will inevitably outstrip the individual's ability to keep pace with technology. In the words of the Foundation for Information Policy Research (FIPR):

> "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" (p 211).

6.7. There were many other expressions of a similar view. We have already drawn on Bruce Schneier's arguments that ISPs should do more to protect individuals. He summed up his position by reference to his mother: "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" (Q 529).

6.8. Elderly parents cropped up several times in our inquiry. Professor Handley said, "I do use e-banking but I have specifically told my parents not to … 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" (Q 694). Professor Anderson (who chairs the FIPR), commenting on the complexities of software design, said "Ultimately, when trying to design such things, you are not designing for geeks because geeks can look after themselves. I always ask myself … 'Well, what about my mum?'" (Q 691). More optimistically, Andrew Cormack said that "I taught my parents how to use [the Internet] safely and that was fairly painless" (Q 992).

6.9. Such comments mask a real demographic change of the last decade, following on from the development of the World Wide Web, and Microsoft's inclusion in the late 1990s of an easy-to-use web browser as standard with its operating systems. We began this Report by noting that Internet use in the United Kingdom grew from 2000–2007 by 144.2 percent. A significant part of this growth is made up of older people—according to the *Oxford Internet Survey*, from 2003–2005, Internet use among pupils and the working population remained almost entirely flat, but among the retired it rose from 22 to 30 percent[26]. As the population continues to age there is every likelihood that "silver surfers" will make up an even larger proportion of Internet users. Education, as Roy Isbell of Symantec noted, will increasingly need to "target that demographic" (Q 452).

6.10. This is not to say that the stereotype of the elderly, gullible and technically incompetent Internet user is justified—gullibility and lack of technical know-how will be found in individuals in every age cohort. The key point is that the rate of growth in Internet use across society means that there are bound to be many individuals, of all ages, using the Internet to bank, shop, or send and receive email, without having high levels of IT skills.

Awareness vs knowledge

6.11. There are two key aspects to improving the ability of individuals to manage online security. One is to promote awareness of the risks online; the second is to instil knowledge of how practically to manage them. Both are necessary—one without the other is of little use.

6.12. Currently the picture is disjointed. Evidence from Professor Steven Furnell and Dr Andy Phippen, of the Network Research Group at Plymouth University, highlighted a very high level of understanding of basic terms such as "virus", "firewall" or "Trojan horse". However, it is less clear how far this

---

26 The Internet in Britain: The Oxford Internet Survey (May 2005), p 51: http://www.oii.ox.ac.uk/microsites/oxis/.

self-reported "understanding" of general risks translates into detailed understanding of specific risks and counter-measures. In hands-on trials the Plymouth survey showed that only 73 percent of users were able to determine the security settings level within their web browser, while only 33 percent were able to determine whether communication with a specific web page was using a secure connection (p 383). Even those who described themselves as "advanced" Internet users (and had academic qualifications relating to IT and experience of Internet security) were by no means uniformly able to perform these tasks.

6.13. Such findings were echoed by several witnesses. According to the Royal Academy of Engineering, "despite fairly high levels of awareness and concern about threats in general, the level of awareness of the actual threats is fairly low" (p 427). EURIM concluded that "awareness is less of a problem than conflicting and impractical advice and guidance", and expressed concern at the "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" (p 370).

6.14. We fully endorse EURIM's point, that raising awareness or risks without developing the knowledge and skills needed to manage such risks could undermine confidence in the Internet. The Government's evidence, however, blurs this distinction. It identifies "information, understanding and appropriate training" as "among the primary challenges in tackling the growing risk of Internet security threats". It also draws attention to initiatives "to raise public awareness of e-crime and the basic steps users can take to protect themselves" (p 5).

6.15. We have already drawn attention to the findings of a survey sponsored by the Government's "Get Safe Online" website, showing that 21 percent of people thought e-crime was the type of crime they were most likely to encounter, and that e-crime was feared more than mugging, car theft or burglary. These findings are clearly out of proportion to the real risk—but it may be that the Government's well-intentioned efforts to raise "awareness" of e-crime, without paying enough attention to the ways in which individuals or businesses can protect themselves against it, are actually making the problem worse.

Sources of information and advice

6.16. To meet the challenges of public understanding, according to the Government, "simple, clear advice from one source is required". They go on to identify the "Get Safe Online" website, bringing together Government, industry and law enforcement, as providing such a source. However, a few paragraphs further on, the Government also note that "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) [*sic*], Bank Safe On Line, IT Safe and Fraud Alert" (p 5).

6.17. There is thus a contradiction in the Government's position. On the one hand they are rightly conscious of the need to provide a single, integrated source of information and advice on Internet security—Vernon Coaker described co-ordination of information as "something we need to become smarter at" (Q 893). But at the same time the sources of information are diverse and overlapping:

- Get Safe Online[27] is the closest thing in this country to a comprehensive, unified source of information on online security and safety. It is sponsored jointly by the Government, the Serious Organised Crime Agency, major IT companies such as Microsoft and BT, and companies from the financial services sector such as HSBC.
- The Government also provide other services, including IT Safe[28], which sends email alerts to home and business users, and a Home Office website dedicated to identity theft[29].
- The banking industry, through payments service APACS, sponsors Bank Safe Online[30], as well as a separate website devoted to card fraud, Card Watch[31].
- The Metropolitan Police Service has created the Fraud Alert site[32], to which victims of e-crime can forward complaints and fraudulent emails—though this is directed primarily at residents of London.

6.18. The Internet is open to all—it will never be possible wholly to prevent the multiplication of sources of advice on security. However, it is clear that the Government should be seeking, in collaboration with public and private sector partners, to provide a single, coherent source not just of information, but of realistic advice on the practical steps that individuals can take to manage risk. In many respects the Get Safe Online website already provides such advice in exemplary fashion. However, since its launch in late 2005 a number of the original sponsors (including companies listed in the Government memorandum, such as Lloyds TSB, Dell and MessageLabs) appear to have withdrawn their sponsorship. This is worrying: the site needs a higher profile and the authority that would come from a wider range of private sector sponsors. To achieve this it needs stronger, high-level political endorsement.

The role of Ofcom

6.19. The regulator of the communications industry, Ofcom, is notable by its absence from the list of sponsors of Get Safe Online, despite the fact that Section 11 of the Communications Act 2003 gives Ofcom a statutory duty to promote "media literacy". Ofcom defines media literacy as "the ability to access, understand and create communications in a variety of contexts" (p 322)—a definition with which we have no quarrel. However, Ofcom's action hitherto appears to have been limited to a "media literacy audit", focusing on issues such as attitudes to the disclosure of personal information online and the blocking of inappropriate content. Ofcom's evidence did, however, state that "in 2007–08 Ofcom will place a much greater emphasis on media literacy" (p 323).

6.20. In oral evidence Tim Suter, Ofcom Partner for Content and Standards, accepted that it was part of the regulator's remit "to help consumers to both

---

27 http://www.getsafeonline.org/.

28 http://www.itsafe.gov.uk/.

29 http://www.identitytheft.org.uk/.

30 http://www.banksafeonline.org.uk/.

31 http://www.cardwatch.org.uk/.

32 http://www.met.police.uk/fraudalert/.

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" (Q 1025). But when pressed on how Ofcom had in fact gone about this task, he referred only to the survey and to the new kite mark on content control software (for which see above, paragraph 3.17).

6.21. Thus Ofcom's formal definition of "media literacy" ("the ability to access, understand and create communications in a variety of contexts") is extremely broad, and would certainly encompass technical security online (for example, the ability to spot a phishing email). Yet its interpretation of "media literacy" in practice is far narrower, and wholly content-focused. It appears to have take no steps at all in the area of technical Internet security. Not only does it not sponsor Get Safe Online, but anyone seeking information from the Ofcom website on, for instance, spyware, will simply be told to "ask your ISP for more advice"[33].

6.22. Ofcom's narrow interpretation of "media literacy" is puzzling. Section 11 of the Communications Act 2003 defines "media literacy" in terms of the public's understanding of "material published by means of the electronic media". Material is further defined as being "published" if it is "distributed by means of an electronic communications network to members of the public or of a section of the public".

6.23. We have already noted that the way in which information transmitted via the Internet is broken down into packets of data means that the superficially plausible distinction between "content" and what can loosely be described as "code" collapses. It follows that Section 11 can be interpreted to cover a very broad range of data distributed by means of the Internet, not just what might be loosely defined as "content". Ofcom's remit is thus in reality so broad as to encompass all aspects of media literacy—technical competence in managing operating systems and security software as well as the ability to control "content" safely.

6.24. In light of these considerations, we can only agree whole-heartedly with the words of the Minister, Margaret Hodge MP: "Could we have a step change in Ofcom's performance around its media literacy duties? I think the answer has to be, yes" (Q 868).

Education

6.25. There is a clear need for information and advice to be made available by means of websites such as Get Safe Online. However, the provision of such information has its limitations: as the British Computer Society commented, "Web-sites run by both Government and the private sector … are 'pull technology' and require the user to go looking for the information they contain" (p 352). Education too is needed.

6.26. Information communications technology (ICT) is already a compulsory element of the school curriculum in Key Stages 1–4, with national qualifications, including GCSEs and a GNVQ, available at age 16—though no part of the national ICT curriculum has hitherto included a security component[34]. This omission is currently being rectified, and, as Home Office

---

33 See http://www.ofcom.org.uk/consumeradvice/internet/security/spyware/.

34 See http://www.nc.uk.net/webdav/harmonise?Page/@id=6004&Subject/@id=3331.

Minister Vernon Coaker MP told us, the Qualifications and Curriculum Authority (QCA) is "looking at ensuring that online safety is part of the ICT study arrangements for Key Stage 3 from September 2008" (Q 892). This is a welcome, albeit arguably overdue, development. As Mr Coaker continued, it is essential "to teach [pupils] that this is a fantastic tool which opens up all sorts of opportunities and educational possibilities, but it is also something … which can be misused".

6.27. At the same time, it is essential that schools themselves should have secure IT systems in place, so that children are not exposed to risks in the school environment. The arrangements for achieving such security are improving, and the National Education Network (NEN) commented that the Government-sponsored agency Becta was "undertaking excellent work in moving UK schools towards a standards-based approach to the design of IT systems" (p 407). Network connections for schools are typically provided by the 10 Regional Broadband Consortia, formed as part of the Department for Education and Skills' Regional Broadband initiative. East Midlands Broadband Consortium, which submitted evidence to this inquiry, provides connectivity to 2,100 schools (p 365).

6.28. However, NEN also expressed concern at possible inconsistencies in interpretation of network design by technical staff in schools, as well as at the implications of increased devolution of funding to local level. Andrew Cormack, who has been involved in revising the ICT curriculum, noted that "Getting teachers, not just to teach Internet security one hour a week but to themselves behave correctly, that is hard" (Q 992). As in other areas of the curriculum, achieving consistently good practice across all schools will be a huge challenge.

6.29. Moreover, teaching online security to school pupils as part of the ICT curriculum will not in itself be sufficient. It is worth recalling that the explosion in use of the World Wide Web dates back only to the mid-1990s; anyone beyond their late 20s is likely to have learned to use the Internet not at school, but as an adult. While the QCA regulates courses in ICT targeted at adults, reaching the bulk of the adult population is a far greater challenge.

6.30. The scale of this challenge was highlighted by a 2006 survey by NCH (formerly National Children's Homes). Focusing on child safety (an issue which we discuss in more detail below), NCH highlighted what it called "alarming discrepancies" between the level of understanding of the Internet of children and that of their parents. For instance, it claimed that a third of children used blogs, while two thirds of parents did not even understand what a blog was, and only 1 percent of parents believed their children used blogs.[35]

6.31. Attempts have already been made to close these gaps. For instance, Tim Wright, of the Home Office, asked whether schools could run voluntary evening classes for parents, told us that "Some schools have tried but, anecdotally, take-up amongst parents has often been poor … 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." Jim Gamble, Chief Executive of the Child Exploitation and Online Protection Centre (CEOP), which has close links to schools, was in favour of

---

[35] Get I.T. safe: Children, parents and technology survey 2006 (NCH)—see http://www.nch.org.uk/uploads/documents/Get%20IT%20safe%20report.pdf.

"demystifying" the technology for parents. For him the question was "how do we engage them in a way that helps them develop a better understanding?" He suggested using the technology itself to communicate with parents, for instance by sending school reports by email as well as in writing (Q 201).

6.32. More generally, we fully endorse the statement by UKERNA (which operates the JANET network linking universities, Research Councils and regional schools networks) that "all opportunities to raise awareness, skill and confidence levels of users of all ages need to be taken". UKERNA went on to highlight the possibility that "children who learn safe practice at school should be encouraged to teach their parents and grandparents at home" (p 299). Such approaches will require creativity on the part of individual communities, schools, businesses and charities—it is not necessarily an area for direct Government intervention. UKERNA, for instance, singled out for praise the interactive "Know IT All" site developed by the charity Childnet International.[36]

Personal safety online

6.33. We began this Report by distinguishing between Internet security—the means of controlling the uses to which PCs or other interconnective devices, and the information stored on them, are put—and Internet safety—that is, personal safety, the avoidance of direct physical or psychological harm that may affect individuals as a result of their actions online. The first of these issues was from the start the focus of this inquiry, and of most of the evidence we received. However, we also received evidence on the second issue, which is discussed briefly in the following paragraphs.

6.34. This distinction is of course to some extent artificial, as any victim of crime, including online fraud or identity theft, may suffer personal harm—stress and anxiety, at the very least—in addition to financial loss. At the same time it allows us to separate out from the main subject-matter of this Report particular issues to do with online behaviour, child protection, and social networking online.

6.35. The first point to be made is that the Internet has been of enormous value in facilitating new forms of communication. No-one would have predicted 20 years ago the way in which email has become a mainstay of social interaction; in the mid-1990s few had heard of SMS, now an industry worth over $80 billion per annum; five years ago no-one would have predicted the explosion of social networking, Instant Messaging and VoIP. New technologies and opportunities continue to emerge.

6.36. But this rate of innovation has also been bewildering. It takes time for people to develop norms of behaviour appropriate to new forms of communication. In the physical world many such norms are well-established: when meeting someone for the first time, an individual identifies various signals to do with facial expression, eye contact, tone of voice, or physical gestures, and, according to the particular cultural context, knows how to react appropriately. Or, when crossing the road, the individual observes familiar rules to avoid accidents. Although norms have evolved in the online world,

---

[36] See http://www.childnet-int.org/kia/default.aspx.

they are nothing like as sensitive or as effective. The risk of misunderstanding, misrepresentation or exploitation is constant.

6.37. Moreover, even though we live in an era of increasing concern over data protection and privacy, the wholesale disclosure of personal information online has become commonplace. Although attention hitherto has focused on the risk to children of such indiscriminate disclosure of personal information, in reality every Internet user, young or old, faces a degree of risk that this information will be abused by others.

6.38. Software designers are increasingly focusing on the issue of identity management online. In the course of our visit to Redmond we met Kim Cameron, Microsoft's Identity and Access Architect, and discussed Windows CardSpace, which seeks to provide a unified system for online identity management via end-user machines. This is now available in the Windows Vista operating system. The evidence submitted to this inquiry by the small software development company Edentity Ltd outlines a web-based system of identity management known as "Personal Information Brokerage"—while also lamenting the lack of interest in the concept shown by the Government.

6.39. But notwithstanding the technological solutions that might be developed to facilitate identity management online, fundamental aspects of online behaviour will also need to change. The key contributors to online risks were usefully summarised in private briefings given to us by Internet safety consultant Linda Criddle:

- Lack of knowledge;
- Carelessness;
- Unintentional exposure of or by others;
- Flaws in technology—for instance, in the services offered online;
- Criminal acts.

6.40. Linda Criddle was emphatic that the IT industry and businesses operating online should take their share of responsibility for reducing risk in all these areas. Even risks arising from carelessness, which might seem to be a purely individual responsibility, could be mitigated if software products were designed with detection tools that could spot and alert users to characteristic acts of carelessness, such as disclosure of personal information without adequate security. The key was that products should be developed in such a way as to educate consumers about risks and to provide them with the tools to manage these risks.

6.41. Ms Criddle's most scathing criticisms of corporate failure were directed at social networking sites. For instance, she identified several points in the sign-on process for social networking site MySpace (now owned by News Corp), which appeared to encourage or reward the disclosure of personal information—real names, email addresses, photographs, and so on. But social networking sites were not the sole offenders. Security tools on the Microsoft Network (MSN) were also inadequate—for instance, content filtering offered by the MSN network screened only external content, not content generated by the network itself.

6.42. The sorts of issues raised by Linda Criddle are of particular concern to parents. Jim Gamble, Chief Executive of CEOP, noting that "a parent may not understand what a social networking site is", asked, "would you allow

your child to wear a billboard … 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." He too argued that the solution was education: "educating people and simplifying and demystifying … the technology" (Q 222).

6.43. Jim Gamble focused in particular on the formal education system. CEOP has not only developed extensive links with schools, but has also rolled out an education campaign targeted at one million pupils. John Carr, Executive Secretary of the Children's Charities' Coalition on Internet Safety, also focused on schools, though highlighting the difficulties in reaching parents by this means, and concluding that "we also need to find other ways of reaching parents" (Q 243). We agree. It is essential to reach young people through schools. However, we also believe that the more holistic approach described by Linda Criddle, building education into the products developed by industry and business, is vital to supplement formal education.

6.44. We are pleased to observe that to some extent the Government are already moving in this direction. For example, we have previously noted that the regulator Ofcom, with Government backing, has developed a BSI kite mark for content control software, and we have recommended that further kite marks be developed for secure Internet Services. This approach, emphasising industry self-regulation, but providing incentives by means of formal recognition of best practice, could also be extended in the field of personal safety online.

6.45. The Government's view, summarised by Tim Wright, is that "self-regulation is the best approach" (Q 203). John Carr also argued that "self-regulation is always going to be a better approach because it is more flexible and quicker"—though conceding that if self-regulation did not deliver, "the Government will step in and legislate" (Q 248). We agree. Governments are not well-placed to intervene directly in an area as fast-moving and diverse as social behaviour online—they cannot design or identify technological solutions, and they cannot judge the rights and wrongs of the personal behaviour of individuals. However, they can collaborate with industry in agreeing general standards of best practice in such areas as the design of social networking sites, and in awarding recognition (in the form of kite marks) to those that observe these standards.

Recommendations

6.46. **The Government-sponsored Get Safe Online website already provides useful information and practical advice to Internet users, but its impact is undermined by the multiplication of other overlapping websites. We recommend that the Government provide more explicit high-level political support to the Get Safe Online initiative and make every effort to recruit additional private sector sponsors. If necessary, the site should be re-launched as a single Internet security "portal", providing access not only to the site itself but acting as a focus and entry-point for other related projects.**

6.47. **We agree with the Minister that there needs to be a "step change" in the way the regulator Ofcom approaches its duties in relation to media literacy. We recommend that Ofcom not only co-sponsor the**

Get Safe Online project, but that it take on responsibility for securing support from the communications industry for the initiative.

6.48. **We further recommend that, in addition to the new kite mark for content control software, Ofcom work with the industry partners and the British Standards Institute to develop additional kite marks for security software and social networking sites; and that it continue to keep under review possible areas where codes of best practice, backed up by kite marks, might be appropriate.**

6.49. **We recommend that the Department for Children, Schools and Families, in recognition of its revised remit, establish a project, involving a wide range of partners, to identify and promote new ways to educate the adult population, in particular parents, in online security and safety.**

CHAPTER 7: POLICING THE INTERNET

Overview

7.1. We have made many recommendations designed to improve the security of those using the Internet. But whatever improvements are made, there will always be those who will abuse the Internet and its users. No security system is ever perfect, and certain individuals will inevitably seek to profit either from poor technical security or the ignorance and gullibility of other users. The last—but arguably most potent—defence against these "bad guys" is effective law enforcement. If they can be caught, prosecuted, convicted and punished appropriately, then the "bad guys", instead of operating with impunity, will face a genuine deterrent, and the hundreds of millions of law-abiding Internet users around the world should be able to communicate or conduct their business online with less fear that they will become victims of crime.

7.2. However, we have heard considerable scepticism over the capacity of the police and the criminal justice system in this country to enforce the law. In the words of the Federation of Small Businesses, "Anecdotal evidence from members tells us that the police do not seem to have anywhere near the capability necessary to respond to these types of crime effectively" (p 377). It is essential that this perception be corrected, but for this some fundamental problems, legal, technical and administrative, will have to be overcome:

- There is, as we have already noted, no legal definition of "e-crime", nor are data on the incidence, investigation or prosecution of e-crimes (that is to say, crimes committed by means of or with the assistance of the use of electronic networks) collected.
- There are huge technical challenges in investigating e-crimes. The examination of IT equipment, hard disks, mobile phones or other devices, is highly specialised, time-consuming and resource-intensive. Moreover, the structure of the Internet and the difficulty of tracing the true source of particular packets of data present huge challenges in investigating offences.
- The global nature of the Internet means that frauds committed on individuals in the United Kingdom may be perpetrated by criminals in Eastern Europe, using servers based in North America or the far East, and so on. No law enforcement agency can combat e-crime effectively in isolation, but the mechanisms for international co-operation are inefficient and slow-moving.

The legal framework

7.3. In Chapter 2, while considering data collection, we drew attention to the lack of an agreed definition of "e-crime". We recommended that the Home Office establish a system to identify within overall crime statistics offences committed by means of or with the assistance of electronic networks, so as to facilitate data collection in future. In the following paragraphs we examine the legal framework for e-crime in more detail.

7.4. There is general agreement that crimes committed online—e-crimes—may be considered under two broad headings. As Sharon Lemon, of the Serious

Organised Crime Agency (SOCA), told us, there is "the type of crime that can now be committed because technology exists which formerly could not be committed", and then there is "traditional crime moving on-line … traditional criminals using and exploiting technology" (Q 1034). The majority of crimes committed online fall into this second category of old crimes using new technology—as Tim Wright of the Home Office told us, "Most e-crime is a form of traditional crime like fraud, theft or extortion" (Q 2).

7.5. It follows from this that most crimes committed online constitute well-established offences under the criminal law. Problems in the application these existing offences to the online world have been addressed as they arose. For instance, the Fraud Act 2006 rectified one notable lacuna, summarised by Professor Walden as "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" (Q 368).

7.6. Crimes falling under Sharon Lemon's first heading—crimes that can only be committed because the technology exists—now also appear to be covered by the criminal law. In particular, the recent amendments to the Computer Misuse Act 1990 (CMA) updated offences relating to unauthorised access to computer material, actions intended to impair the operation of computers, and the manufacture or supply of equipment intended to be used for such purposes. These offences now cover computer-specific offences such as distributed denial of service (DDoS) attacks, which were not previously in themselves criminal offences (although using the threat of a DDoS attack to extort money would have been an offence). However, in light of further amendments to be introduced by the Serious Crime Bill, currently before Parliament, the Government have decided not to bring these changes into force until 2008.

7.7. In light of these recent changes to the legislative framework, there was broad agreement among our witnesses that the criminal law now adequately covered the range of offences that could be committed online. Commander Sue Wilkinson of the Association of Chief Police Officers described the legal framework as "entirely adequate" (Q 1038); Nicholas Bohm was also "not conscious of significant legal gaps" (Q 368).

7.8. However, we have two reservations. The first of these concerns the legal status of botnets—which are typically the vehicle for delivering spam or DDoS attacks. We asked the Minister, Vernon Coaker MP, whether it was illegal to purchase the use of a botnet. He summarised the position as follows: "No, it is not illegal to actually purchase it … 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" (Q 837).

7.9. In supplementary written evidence, the Home Office refined the Minister's answer. In essence the analogy with knives was confirmed—hiring a botnet is illegal if it is done in order to commit one of a number of possible offences, either under the CMA (as amended), the Fraud Act 2006, or a range of other statutes. However, hiring a botnet for legal purposes is not in itself a statutory offence, although the person hiring the botnet for ostensibly legal purposes (such as spamming) might in principle be prosecuted either under

the general conspiracy provision found in section 1 of the Criminal Law Act 1977, or under the common law offence of incitement (p 277).

7.10. On the other hand, "recruiting" a botnet—that is, installing code on a computer without the knowledge or authorisation of the owner, and thereby modifying its operation—constitutes an offence under one or more sections of the CMA. However, the degree to which, within the criminal underworld, those who recruit botnets are the same or differ from those who subsequently operate them and offer them out for hire, is unclear.

7.11. More generally, we question the Minister's analogy with knives. A knife *per se* can be used for many legitimate purposes, but the sale or possession of certain kinds of knife (essentially those designed with criminal uses in mind), or the sale of knives to certain categories of people (typically those under 16 years of age) could be illegal under one of a range of statutes, including the Dangerous Weapons Act 1959, the Criminal Justice Act 1988 and the Knives Act 1997. The fact that such knives could in principle be used for lawful purposes does not make their sale legal.

7.12. Similarly, although a botnet could in principle be used for legal purposes, it is inherently designed for criminal uses, and can only exist by virtue of criminal acts by those who recruited it. We would therefore see considerable advantages if the criminal law, for the avoidance of all doubt, were explicitly to criminalise the sale or purchase of the services of a botnet, regardless of the use to which it is put.

7.13. Our second, overlapping reservation, is over the framework for prosecuting spammers, who are typically the customers for botnet operators. From discussions in Redmond with Aaron Kornblum, Senior Attorney at Microsoft, it was clear that Microsoft, AOL and others have made significant progress in the United States in prosecuting spammers, assisted by the fact that both federal and state laws permit companies to launch third-party actions on behalf of their customers. Nicholas Bohm also commented that such actions were "sustainable on a much more simple basis" in the United States than in the United Kingdom, and suggested that "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" (Q 406).

7.14. Written evidence supplied by the Government subsequently suggested that Microsoft had in fact brought two "third-party" actions in the United Kingdom against spammers. However, neither appeared to be a third-party action in the American sense, that is to say, an action brought by the company on behalf of and in the name of its customers:

- In one case, brought under regulation 22 of the Privacy and Electronic Communications (EC Directive) Regulations 2003, Microsoft established that as a provider of email services it had itself suffered damage as a result of the spammers actions. The issue of whether Microsoft was entitled to bring an action under the regulation was explicitly covered by the judge in this case, Mr Justice Lewison: "the domestic regulations were made in order to conform with the provisions of the Directive and part of the policy of the Directive was, in my judgment, to protect the providers of electronic communications' systems. Consequently, I am satisfied that

Microsoft is within the class of persons for whose benefit the statutory requirement was imposed."[37]

- In the second case the spammer, by using spam to attract custom to a pornographic website, was in direct contravention of Microsoft's terms and conditions.

We are therefore not persuaded by the Government's conclusion that "third party legal action is another viable approach to addressing the spam problem" (p 275).

7.15. The Government also pointed out—which we fully acknowledge—that the number of spammers based in the United Kingdom is small compared with that in the United States. They drew attention to research by the anti-spam initiative Spamhaus, showing that only one United Kingdom-based spammer appears on the Register of Known Spam Operations (a list which at the time of writing contains 133 spam operations). However, we see no reason for complacency in such a fast-moving sector.

High volume, low denomination crime

7.16. Since the existing legislative framework covers "traditional" offences committed by electronic means, it follows that the "bad guys", if caught, can be prosecuted for offences such as fraud or extortion. However, this reliance on traditional offences has some possibly unintended consequences. For instance, the use of electronic networks for the commission of an offence, and implications of this, are not necessarily factored in either by the police, when initiating investigations, or by the courts, when sentencing those found guilty.

7.17. To take a hypothetical example, if an individual makes a complaint to the police that they have been the victim of online fraud, losing a few tens or hundreds of pounds, it may appear to be a minor crime, not meriting investigation—particularly as the offender could be anywhere in the world. The problem was vividly described by Garreth Griffith, of eBay: "What happens on eBay tends to be lower-value, higher-volume types of things. When we try to get police engaged, sometimes they say … If it is not over 'x' threshold—thousands of pounds, or whatever it is—we can't help you" (Q 601).

7.18. But if the crime has been committed online, the chances are that thousands or millions of other individuals have been similarly targeted. This is a consequence of the basic economics of e-crime. As Professor Anderson noted, the "bad guys" engage in "volume crime for low denomination transactions" (Q 703). Email is free: anyone who hires the use of a botnet can, at very low cost, send millions of phishing emails or advertisements for bogus medications. If only a tiny proportion of recipients respond the operation quickly becomes hugely profitable. In other words, the individual crime, as reported to the police, has to be scaled up by a factor of several thousand before the true scale of criminality can be guessed at.

7.19. It is therefore crucial that the criminal justice system, at every level, possesses the information and the understanding to be able to seek and detect patterns

---

[37] *Microsoft Corporation v Paul Martin McDonald* [2006] EWHC 3410 (Ch), [2006] All ER (D) 153 (Dec). See http://www.juriscom.net/documents/highcourtjce20061212.pdf.

of criminality, and, where necessary, to aggregate thousands of individually small crimes to build up a picture of the true scale of criminality.

Reporting procedures

7.20. The hypothetical example just cited highlights the first stage of an investigation, the initial report of a crime, which the victim is normally required to make at their local police station. However, it is clear from the previous section that in the case of e-crime local police forces are not well placed, on the basis of isolated reports of what may appear to be petty frauds, either to assess accurately the scale of criminality involved or to reach a judgment on whether to launch an investigation and what resources to devote to it. One way to overcome this problem would be to use the Internet itself to develop a central online reporting system for e-crime—as has happened in the United States.

7.21. At the Department of Justice in Washington we heard the familiar story of individually minor crimes being reported to local police, typically not meriting investigation or federal prosecution. In response the Federal Bureau of Investigation (FBI), having identified e-crime as its number three priority, after international terrorism and espionage, has developed a central referral mechanism for Internet related crime, by means of the Internet Crime Complaint Center (IC3)[38] website. This facilitates central logging of crime reports, which are then analysed and correlated. Individually minor crimes can be aggregated until they reach the threshold for launching federal prosecutions.

7.22. Our discussions at the FBI's Regional Computer Forensic Laboratory in Silicon Valley fully endorsed the value of the Bureau's approach. Special Agent Shena Crowe told us that the IC3 site was logging an average of some 20,000 complaints a month. Median losses reported in 2005 were just $424, but total losses reported on the site in that year totalled $183.12 million. Subsequently these data were updated in the IC3 Internet Crime Report for 2006, which confirmed a total of just over 207,000 complaints in that year; over 86,000 of these were referred to federal, state or local law enforcement agencies for further investigation. Losses from the latter were put at $198.44 million, with median losses rising to $724[39]. This sounds like a small sum—but to the individuals concerned it may be a major loss.

7.23. Reports to the IC3 site are still voluntary, nor are they confined to crimes perpetrated in the United States (and we have already noted a reporting bias in paragraph 5.09 above), so the relationship between these figures and the actual scale of e-crime is unclear. However, the IC3 figures do demonstrate the value of a central system that can "triage" large numbers of complaints, prioritise them and finally allocate them to the appropriate agencies for further investigation.

7.24. No comparable system exists in the United Kingdom. Instead the responsibility for logging reports of e-crime remains with individual police forces. We have referred previously to the Metropolitan Police Service's (MPS) "Fraud Alert" website, but we learnt in the course of our visit to the Metropolitan Police at Cobalt Square that unlike IC3 the Fraud Alert site

---

38 See http://www.ic3.gov/.

39 See http://www.ic3.gov/media/annualreport/2006_IC3Report.pdf.

does not have an automated system for processing reports of fraud—the software to automate the site would cost of the order of £40,000. In the absence of this modest funding, all reports are collated manually, and any attempt to publicise the site would risk attracting more reports than the staff could process. The impression we drew from our visit was of highly committed and skilled staff doing their best to cope in an under-resourced and under-valued environment.

7.25. This could change. Earlier this year senior officers from the police and SOCA visited IC3. One of these officers, Commander Sue Wilkinson of the MPS, accepted that we had "a lot to learn" from IC3 (Q 1052). At the same time, the introduction of a comparable service in this country would need to be managed in such a way as to avoid overlap with "the new strategic fraud authority and the new potential national fraud reporting centre that is currently being scoped by the City of London Police". Similar views were expressed by Mr Coaker. He confirmed that the Government were "happy to look at" the IC3 model, but also drew attention to the prospect of a central reporting system for fraud. His irreproachable conclusion was that "there needs to be some co-ordination across the whole of this" (Q 808).

7.26. However, in certain key areas the Government's actions appear to have taken us if anything further away from a co-ordinated approach to e-crime reporting. Anyone logging onto the Fraud Alert site is faced with the following instructions on the homepage: "Please send all banking related phishing emails to reports@banksafeonline.org.uk. Queries related to Paypal or Ebay should be sent to spoof@paypal.co.uk and spoof@ebay.co.uk respectively." This is followed by an optimistic request to "Please copy us into any emails that are sent to these organisations"—although it is necessary to navigate to another page to locate the Metropolitan Police email address.

7.27. The fact that those seeking to report online frauds are specifically discouraged from reporting these crimes to the police is attributable to new guidelines issued to police forces by the Government with effect from 1 April 2007. The Minister, speaking before the new guidelines came into force, explained them as follows: "from 1 April people experiencing … 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 … 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" (Q 826).

7.28. This is an extraordinary argument, placing the onus on the banking industry to take decisions on which crimes should or should not be reported to the police (and if so, to which force)—and what will or will not, as a result, appear on the crime statistics. It appears to overlook the obvious possibility that commercial factors might influence the banks' decisions on whether or not to report crimes to the police—that, in the words of Ross Anderson, they have "an institutional incentive to downplay the amount of fraud" (Q 678).

7.29. A slightly more persuasive argument in defence of the Government's position was advanced by Geoff Smith, of the DTI. He claimed that the issue was "essentially about 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 … try and stop the cash transfers and they try and limit the damage through that. So … 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" (Q 833).

7.30. We also acknowledge that law enforcement agencies have thrown their weight behind the new guidelines. Commander Wilkinson described them as "very helpful". She continued, "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" (Q 1098).

7.31. Commander Wilkinson's comments are revealing—they demonstrate that the doubts expressed by a number of witnesses to this inquiry (for instance, by Garreth Griffiths of eBay, whose remarks are quoted above), over the capability of the police to collect, collate and investigate reports of e-crime, are fully justified. The proper response, we believe, would be to invest in developing the capacity of the police and law enforcement agencies, so that they could take on this crucial task—instead of which, the Fraud Alert team at the Metropolitan Police cannot even afford to spend £40,000 on software to automate the processing of e-crime complaints.

7.32. In marked contrast, the United States is moving in the opposite direction. When we visited the Federal Trade Commission (FTC), which receives over 450,000 complaints of identity theft alone each year, we were told that a new reporting system was being introduced, requiring victims of identity theft (which would include thefts from online bank accounts) to file a police report as the first step in making a complaint; this would in turn trigger an investigation by financial institutions. Indeed, the Interim Recommendations of the President's Identity Theft Task Force, which appeared in late 2006, proposed that the FTC should develop "a universal police report, which an identity theft victim can complete, print, and take to any local law enforcement agency for verification".[40]

7.33. We see no reason why a similar system in this country should be particularly bureaucratic, time-consuming or costly to implement. The logging of a complaint by the police could simultaneously alert the banks. At the same time, victims would be reassured that the crimes committed against them had been formally acknowledged and recorded, rather than disappearing into the banking system.

7.34. Ultimately the new reporting system is likely to be judged by its results. It is too early to tell what these will be—but the omens are not good. On 21 June, for example, the BBC reported a dramatic fall in reports of fraud to police forces, with two smaller forces, Gwent and North Yorkshire, having received no reports since the new guidelines came into effect.[41] It is very unlikely that this drop in reported frauds reflects a real change in criminality—the risk is that while lower reporting will make the crime statistics look better, e-crime will continue to grow out of sight of the police and the public.

---

[40] See http://www.idtheft.gov/about.html.

[41] See http://news.bbc.co.uk/1/hi/business/6224912.stm.

The structure of law enforcement

7.35. Assuming that a complaint is made and recorded by the police, do they, or other law enforcement agencies, have the skills, resources and powers necessary to investigate it?

7.36. The first key point is that the 43 police forces across England and Wales are essentially autonomous. Chief Constables report to police authorities, and inevitably respond to local needs and priorities. The size of police forces also varies hugely, from the Metropolitan Police Service, with over 30,000 officers, to forces with fewer than 1,000 officers, such as the City of London Police or Warwickshire Police. The resources available to tackle e-crime, as well as the priority given to it, vary widely from force to force.

7.37. Alongside the police forces is the Serious Organised Crime Agency (SOCA), which in 2006 took over the responsibilities previously exercised by the National Criminal Intelligence Service, the National Crime Squad, along with other agencies. Among the functions absorbed into SOCA were those of the National High Tech Crime Unit (NHTCU), formed in 2001 as part of the National Crime Squad specifically to combat e-crime. At the same time, the creation of the Child Exploitation and Online Protection Centre (CEOP), which is affiliated to SOCA and accounts to the SOCA Board, meant that online child abuse, formerly handled by the NHTCU, no longer fell within SOCA's operational remit.

7.38. These organisational changes have raised a number of concerns. The Confederation of British Industry focused on "the perceived reduction in dedicated police resources to combat computer crime" resulting from the disappearance of the NHTCU (p 194). Microsoft suggested that it was now "unclear how cyber crime and reporting mechanisms are being systematically addressed" (p 94). The FIPR claimed that "the absorption of the NHTCU into SOCA has left a gap in the coverage of level 2 computer crime" (p 212)—that is to say, crime that has impacts across force boundaries, but not necessarily at national or international level.

7.39. Some of these concerns were answered in the course of our inquiry. We note, for instance, that SOCA's board has determined that of the order of ten percent of the Agency's operational effort should be directed against fraud.[42] In evidence Bill Hughes, Director General of SOCA, while acknowledging that the changes might have appeared to show "a lack of interest in e-crime", argued that "the reverse is the case". The creation of a dedicated e-Crime Unit within SOCA (headed by Sharon Lemon, formerly head of the NHTCU), along with the creation of CEOP (thanks to which the Unit's resources were no longer at risk of being diverted into child abuse cases), meant that resources had been "marshalled … in a better way" (Q 1033).

7.40. The situation on level 2 crime is less clear. The first point to be made—put very clearly by Bill Hughes—is that there is no neat dividing line between levels 1, 2 and 3 crime: "There is a danger when talking about levels one, two and three … 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 of activity and understanding" (Q 1054). But at the same time, there have to be robust procedures and organisational arrangements in place for this "continuum" to be workable in practice.

---

[42] See http://www.soca.gov.uk/aboutUs/aims.html.

7.41. Local level 1 crime falls to individual police forces; level 3, national or international crime, is the responsibility of SOCA. Asked who was primarily responsible for investigating level 2 crime, Sue Wilkinson, the Association of Chief Police Officers (ACPO) lead on e-crime, drew attention to the recent proposal by ACPO to establish a national e-crime unit to support individual police forces. At the time of our inquiry this remained under discussion between ACPO and the Home Office—Vernon Coaker commented that the Home Office had "not had the business case yet", and at the time he gave evidence (on 28 March) the Department had "made no commitment with resources" (Q 814).

7.42. When we spoke to Commander Wilkinson a month later, she told us that ACPO now had "the go ahead" from the Home Office. However, no Government funding had been approved, and she was still "in the throes" of preparing a detailed business case. She was optimistic that "a considerable amount of sponsorship will be forthcoming"—indeed, she went so far as to say that potential sponsors were "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'" (Q 1087). However, when asked repeatedly whether a commitment by the Home Office to provide funding would be necessary to unlock this private sector backing, she declined to give a direct answer, simply repeating that she had "no undertakings currently of Government support" (QQ 1059–1063).

7.43. Just before our Report was agreed, on 19 July, the name of the new unit was announced (the "Police Central ecrime Unit") and its projected budget (£4.5 million). However, it appeared that the Government had still made no commitment as to funding. But assuming the new unit does secure funding from Government and private sector sponsors, its role will essentially be to help establish the continuum of which Bill Hughes spoke, between the work of local police forces and that of SOCA and its international partners. Sue Wilkinson confirmed that she and Sharon Lemon were "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" (Q 1054). The successful establishment of the Police Central ecrime Unit, and the agreement of such protocols, appear to be essential if Bill Hughes' vision of a continuum of policing of e-crime is to be achieved.

Police skills and resources

7.44. Even if the organisational arrangements described above fall into place, law enforcement agencies at every level will need skills, knowledge and resources if e-crime is to be investigated effectively. On the one hand, the public have a right to expect that if they report an e-crime at their local police station the officer at the desk will have a general understanding of the kind of crime that has been committed; on the other hand, computer forensics are hugely expensive and laborious, and police investigating major e-crimes will need access to specialised and well-equipped forensic laboratories.

7.45. At a basic level, training and information for all police officers will be increasingly important as interconnective devices proliferate, and their use, whether to commit crime or in normal life, becomes all but universal. At crime scenes, officers need to observe key rules to ensure that the evidence stored on computers or other devices is not contaminated. Computers or laptops should not be started up or searched, they should be disconnected

from routers and modems, mobile telephones should be kept charged so as not to lose data, and so on.

7.46. In the United States we were given copies of an impressive "pocket guide for first responders", issued by the Department of Homeland Security and the United States Secret Service, summarising best practice in a compact, readily accessible form. Sue Wilkinson assured us that ACPO also published "good practice guides", including one covering "computer based electronic evidence and evidence retrieval" (Q 1085). However, we note that the online version of this guide runs to 51 A4 pages[43], in marked contrast to the American guide, which is ring-bound, pocket-sized and waterproof—intended specifically for use by officers at a crime-scene.

7.47. Assuming the police have launched an investigation, there is also the question of the resources and skills required for detailed forensic analysis of computers and other materials that have been seized. Here again we were impressed by the approach adopted in the United States, where the FBI has co-ordinated the development of a national network of 14 Regional Computer Forensic Laboratories. These receive federal funding to support running costs, such as IT equipment and premises, but the staff are largely provided and funded by local law enforcement. In return, the laboratories provide forensic analysis to local police free of charge.

7.48. Clearly, 14 laboratories in a country the size of the United States is not a large number. But at least the model of central provision of the highly specialised facilities recognises the unique challenge posed by computer forensics. Chris Beeson, Director of the Silicon Valley laboratory, told us that the volume of data processed had increased from 40 Terabytes in 2000 to over 1,400 Terabytes[44] in 2005. We question whether it will be possible for all of the 43 police forces in England and Wales to maintain the level of skills and equipment necessary to keep pace with this rate of growth.

7.49. Sue Wilkinson described the creation of such a national network in the United Kingdom as the "ideal scenario"—but conceded it would "take some time to achieve". In the meantime, ACPO had conducted a "very provisional capability assessment" of the 43 police forces, and had "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" (Q 1083). In the longer term, however, the proposed ACPO national e-crime unit was "needed to get standards, policy, training and skills levels standardised across the country" (Q 1085). When the establishment of a national network was put to the Minister, he simply reiterated that he was "waiting for Commander Sue Wilkinson and others to come forward with the proposals" (Q 817).

7.50. Pending the development of a national unit or network specialising in e-crime and computer forensics, ACPO's approach is to "mainstream" e-crime within conventional policing. The rationale behind this approach is to escape from what Sharon Lemon described as "the problem with policing [which] 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" (Q 1034).

---

[43] See http://www.acpo.police.uk/asp/policies/Data/gpg_computer_based_evidence_v3.pdf.

[44] 1 Terabyte = 1 million Megabytes, or 10^{12} bytes.

7.51. Mainstreaming, on the other hand, means adopting an extremely wide definition of e-crime ("the use of networked computers, telephony or Internet technology to commit or facilitate crime"—Q 1036), to emphasise that e-crime is in reality just crime, requiring all police officers, not just the specialists, to acquire a basic level of skills. The objective was summarised by Sue Wilkinson as "not to try to shift everything into specialist units but to raise the level of awareness and capability right the way across the board" (Q 1037).

7.52. The intention behind mainstreaming is laudable, but there is a fundamental contradiction: as we noted in Chapter 2, treating e-crime as conventional crime means that it is impossible to assess its rate of growth, or the cost to individuals or the economy; it also makes it impossible to set policing targets or priorities relating to e-crime. The logical consequence of "mainstreaming" e-crime is that the bulk of e-crime will be subsumed into conventional crime, in which case it will no longer be a distinct policing priority. All that will be left will be the rump of e-crimes that exist only because the technology exists—typically, offences covered by the Computer Misuse Act 1990, as amended.

7.53. A balance has to be struck. We have considerable sympathy with Sharon Lemon's view that specialists are called in unnecessarily to investigate traditional crimes that just happen to involve a computer. But we also believe that if there is enough investment in such specialist resources, the skills developed will be of enormous use in combating not just Computer Misuse Act offences, but the extortion, the frauds, the thefts and all the other conventional offences which currently thrive in the fertile soil of the Internet.

7.54. Another issue raised in the course of our inquiry was the extent to which the police have the resources, and, more critically, the powers to investigate e-crime proactively, through monitoring Internet traffic. As we noted in Chapter 2, and as the FBI confirmed when we visited Silicon Valley, huge volumes of criminal activity are conducted online, sometimes openly, on Internet Relay Chat, Peer-to-Peer (P 2P) or other networks. However, while researchers in the United States, such as Team Cymru, are entitled to monitor such traffic for the purposes of research, US law enforcement agencies are forbidden from doing so unless they have "probable cause".

7.55. In this country, the police are able to monitor online communications, provided that their activity is permitted under the surveillance provisions of Part II of the Regulation of Investigatory Powers Act 2000. On our visit to the Metropolitan Police Computer Crime Unit we met officers who were actively monitoring the online behaviour of paedophiles, a number of whom they had already arrested. However, at present there does not seem to be any monitoring within the UK, even for basic intelligence purposes, of the "underground economy" identified by Team Cymru.

7.56. An alternative approach, put forward by Ross Anderson, might simplify the process whereby investigations are launched. This was for "randomised enforcement". In other words, the volume of e-crime is such that if the police decide to investigate one randomly selected and apparently minor offence, such as a petty online fraud, each month, "you ensure that someone who perpetrates millions of £10 frauds comes into the police sight eventually" (Q 703).

International action

7.57. The nature of e-crime is to cross national jurisdictions. The victim may live in the Home Counties—but the perpetrator could be anywhere in the world. International co-operation between law enforcement agencies and judicial systems is therefore vital.

7.58. We were not able to establish a clear or consistent picture of the state of international co-operation. On the one hand, Sharon Lemon told us that SOCA's e-crime unit had "established some exceptional working relationships with our international partners". She also mentioned a range of international task-forces for particular offences, while Bill Hughes drew attention to the "international liaison network" within SOCA. He also cited "good examples of work for example with the Russian and the Chinese" (Q 1108), while refusing to identify any problem countries.

7.59. In marked contrast, Shena Crowe at the FBI laboratory in Silicon Valley told us that international action was difficult and slow, with requests for assistance often either ignored or subject to barter. She noted that Russia and China were often cited as major sources of international e-crime—Shane Tews at Verisign in Washington also told us that states in eastern Europe and Asia were turning a blind eye to organised criminals operating on the Internet. To add to the confusion, Sharon Lemon also told us that "the current procedures for sharing information and intelligence can be extremely sluggish", while Sue Wilkinson said that "investigations can fall down because of the fact that legislation does not really cover the international challenge" (Q 1038).

7.60. A more concrete description of the difficulties of international action was provided at eBay. The view of Rob Chesnut, Senior Vice President for Trust and Safety, was clear—the best way to deter e-crime was to put the fraudsters in jail. The main impediment to achieving this was the fact that the authorities in some countries simply were not interested in helping investigations. eBay devoted considerable effort to developing relationships with international law enforcement agencies, and had supported over 100 convictions in Romania alone, by providing materials and in some cases by paying for victims to go there to give evidence in person. One of the company's key recommendations was that laws of evidence should be relaxed to make it easier for testimony to be given from outside the country concerned, for instance using written statements or video links.

7.61. It was clear from our visit to the United States that the United Kingdom is seen as a "good partner" in international action on e-crime. Despite this, the United Kingdom has yet to ratify the Council of Europe's 2001 Convention on Cybercrime. This is a matter of concern, particularly as among the provisions in the Convention is a requirement that parties should "afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence" (Article 25).

7.62. When we asked the Minister about the delay in ratification, he confirmed that the Government were "committed to ratifying the … Convention" (Q 804). Certain minor legislative changes were required, and these would be completed by means of the Serious Crime Bill (which at the time of writing was being considered by the House of Commons). However, when

asked about mutual assistance he deferred to his official Stephen Webb, who told us that while the Government had "been generally looking at mutual legal assistance requests" there was "nothing specific in this particular area which is being done" (Q 805).

The courts

7.63. Issues of skills and resources permeate every level of the criminal justice system. Given the rate at which e-crime continues to evolve it was perhaps not surprising that we heard some concerns expressed over the capability of courts to understand the technology underpinning it. Professor Walden, on the basis of several years' experience training prosecutors, claimed that prosecutors had experienced "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" (Q 375).

7.64. Nicholas Bohm argued that "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" would be the most effective way to improve the way the justice system deals with e-crime (Q 368). More concretely, Bill Hughes reflected on "how better we can present the case in court … 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" (Q 1038). However, this proposal might be difficult to reconcile with fact that court proceedings, unlike those of Select Committees, are adversarial. Even expert witnesses, though notionally working for the court, in practice appear on behalf of, and are paid by, either prosecution or defence.

7.65. Nevertheless, Bill Hughes' suggestion of a expert adviser to assist the courts in assessing IT-based evidence is attractive. A case in point is the weight placed by the courts upon the illegal use of credit cards online. As we have previously noted, the introduction of "chip and pin" has led to a rapid increase in online card-not-present fraud. We have also seen Team Cymru's research, showing huge volumes of stolen credit card details being bought and sold online. In the context of data security breach notification we have also noted that one retailer alone, TK Maxx, has since 2005 lost the details of some 45 million cards to hackers. Potentially any one of these cards, belonging to innocent individuals, could be used online for illegal purposes—in transactions relating to terrorism, or to purchase child abuse images.

7.66. This issue led to an exchange of letters between the Committee and, on the one hand, Jim Gamble, Chief Executive of CEOP, and, on the other hand, Duncan Campbell, an investigative journalist, regarding the conduct of Operation Ore, the investigation of over 7,000 individuals in this country whose credit card details were found on a database held by an American company, Landslide Inc, which until it was closed down in 1999 offered access to a number of child abuse websites. When Jim Gamble gave evidence on 10 January, he was asked whether the prevalence of credit card fraud raised any problems in the conduct of such investigations. His response was as follows: "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" (Q 221).

7.67. The Committee then received a letter from Duncan Campbell, who has appeared as a defence expert witness in a number of Operation Ore cases,

flatly contradicting Mr Gamble's statement. The letters that followed, from both Mr Campbell and Mr Gamble, are printed as evidence with this Report (see pp 77-81, 363-365).

7.68. This exchange of correspondence strayed far beyond the remit of this inquiry, and we have no wish to comment on the wider issues raised. However, Mr Gamble did confirm that the Crown Prosecution Service had developed a "response for occasions where no images were found", making use of the common law offence of incitement. He further noted that in such 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". Such issues were assessed "on a case by case basis" (p 78).

7.69. Thus such cases of alleged "incitement" (of which, according to Mr Gamble, there had been 161, with just ten outstanding, though Mr Campbell claimed there were still 2,000 outstanding) rely heavily on evidence of electronic transactions between a suspected individual and a site offering child abuse images online. It is clear us that in assessing such evidence the weight placed upon online credit card transactions will be fundamental. It is essential therefore that judges, prosecutors and magistrates (who decide on applications for search warrants) are able to make intelligent and informed assessments of such evidence.

Sentencing

7.70. Finally we turn to sentencing. Once criminals are convicted of e-crimes it is essential that sentences are robust enough to serve as a deterrent to others. The sentences for technology specific crimes (particularly those under the Computer Misuse Act) are defined in statute. But where "traditional" crimes are committed online, once again the phenomenon of high volume, low denomination crime, creates difficulties. Such crimes are not one-off incidents—if someone is convicted of one online fraud, it is extremely likely that they will have committed many more. We therefore asked a number of witnesses whether the use of a computer to commit an offence could be recognised by the court when sentencing, for instance as an aggravating factor.

7.71. In response, Bill Hughes took the view that the commission of crimes online could feasibly be "reflected in the sentencing, depending on the aggravation factor". He cited as an example the lottery scams which target "the more vulnerable in society"—those who by responding to bogus emails have found themselves on the criminals' "sucker list" (Q 1040). The Government were less sympathetic to this idea, and Stephen Webb, of the Home Office, suggested that "You have to make a case for why it was worse to defraud someone over the Internet rather than sending them the 419 letter[45] by post, or scamming them and meeting them face to face on the street" (Q 28).

7.72. Other aggravating factors that could influence sentencing might include the high level of intrusion involved in crimes committed via electronic networks—for instance, the courts could recognise that making threats by means of text messages or Instant Messaging constituted an invasion of the

[45] The "419 fraud" is a form of advance fee fraud, in which the victim is persuaded to put down a sum of money in anticipation of a much larger gain, which then fails to materialise. The modern manifestation of this ancient fraud emerged in Nigeria in the 1980s—the number 419 refers to the relevant article of the Nigerian criminal code.

home on top of the basic offence committed. Bill Hughes again offered some sympathy, if not direct support, for this view:

> "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 … how do you present this in a court case where you can realise the aggravating factors and the damage that this can cause" (Q 1041).

7.73. In summary, our concern is whether the criminal justice system as a whole has a sufficiently high and consistent level of understanding of e-crime to be able to make balanced, evidence-based decisions. Do police officers across the 43 forces observe consistent best practice in the way in which they handle such investigations? Do magistrates understand the value and the limitations of electronic evidence, in particular evidence of online credit card transactions, so as to be able to judge the appropriateness or otherwise of issuing search warrants? Are judges in the crown courts competent to direct juries in such cases, or to hand down adequate sentences to those found guilty? On the basis of the evidence received in this inquiry, the answer to all these questions currently seems to be "no".

Conclusions and recommendations

7.74. **We recommend that the Government introduce amendments to the criminal law, explicitly to criminalise the sale or purchase of the services of a botnet, regardless of the use to which it is put.**

7.75. **We recommend that the Government, in partnership with the Association of Chief Police Officers and the Serious Organised Crime Agency, develop a unified, web-based reporting system for e-crime. The public face of this system should be a website designed to facilitate public and business reporting of incidents. The back-end software should have the capacity to collect and collate reports of e-crime, identify patterns, and generate data on the incidence of criminality. The website could also serve as a portal to other more specialised sites, for instance on online child abuse or identity theft. It would be an invaluable source of information for both law enforcement and researchers.**

7.76. **As a corollary to the development of an online reporting system, we recommend that the Government review as a matter of urgency their decision to require online frauds to be reported to the banks in the first instance. We believe that this decision will undermine public trust in both the police and the Internet. It is essential that victims of e-crime should be able to lodge a police report and have some formal acknowledgement of the fact of a crime having been committed in exchange. We see no reason why such reports should not be made online, processed and forwarded to the banks automatically.**

7.77. **If these recommendations are to be acted upon, the police service will need to devote more resources to e-crime. We acknowledge the good work undertaken by SOCA and on behalf of ACPO, but within the police skills and forensic capability still vary from force to force.**

While it is vital to raise police skills across the board, rather than just those of specialists, "mainstreaming" is only part of the answer. We therefore recommend the establishment of a network of computer forensic laboratories, under the aegis of the proposed ACPO national e-crime unit, but with significant central funding.

7.78. **We further urge the Home Office, without delay, to provide the necessary funds to kick-start the establishment of the Police Central ecrime Unit, without waiting for the private sector to come forward with funding. It is time for the Government to demonstrate their good faith and their commitment to fighting e-crime.**

7.79. **These recommendations will all cost money. But e-crime is expanding rapidly: the choice is either to intervene now to make the necessary investment, and perhaps to keep the threat to the Internet under control, or to let it grow unchecked, and risk an economically disastrous, long-term loss of public confidence in the Internet as a means of communication for business and Government alike.**

7.80. **We urge the Government to fulfil its commitment to ratify the Council of Europe CyberCrime Convention at the earliest possible opportunity. At the same time, in order to ensure that the United Kingdom fulfils the spirit as well as the letter of Article 25 of the Convention, we recommend that the Government review the procedures for offering mutual legal assistance in response to requests for help from other countries in investigating or prosecuting e-crime.**

7.81. **Finally, we recommend that the Government take steps to raise the level of understanding of the Internet and e-crime across the court system. In particular:**

- **In the context of the prevalence of identity theft and online card fraud, we urge the Government to issue new guidance to the courts, including magistrates' courts, on the reliability of unsupported credit card evidence as an indicator of guilt;**
- **We recommend that the Government review the availability to the courts of independent specialist advice in cases of Internet-related crime;**
- **We believe that the sentence should fit the crime. The nature of e-crime is such that mostly (but not exclusively) small crimes are committed in very large numbers; they also generally involve a high level of intrusion into personal life. Sentencing guidelines should be reviewed in recognition of these realities.**

CHAPTER 8: SUMMARY OF CONCLUSIONS AND RECOMMENDATIONS

8.1. In this Chapter we set out our recommendations and conclusions in full. The numbers in brackets refer to the relevant paragraphs in the text.

Overview: The Internet and Personal Security

8.2. The benefits, costs and dangers of the Internet, are poorly appreciated by the general public. This is not surprising, given the lack of reliable data, for which the Government must bear some responsibility. The Government are not themselves in a position directly to gather the necessary data, but they do have a responsibility to show leadership in pulling together the data that are available, interpreting them for the public and setting them in context, balancing risks and benefits. Instead of doing this, the Government have not even agreed definitions of key concepts such as "e-crime". (2.42)

8.3. We recommend that the Government establish a cross-departmental group, bringing in experts from industry and academia, to develop a more co-ordinated approach to data collection in future. This should include a classification scheme for recording the incidence of all forms of e-crime. Such a scheme should cover not just Internet-specific crimes, such as Distributed Denial of Service attacks, but also e-enabled crimes—that is to say, traditional crimes committed by electronic means or where there is a significant electronic aspect to their commission. (2.43)

8.4. Research into IT security in the United Kingdom is high in quality but limited in quantity. More support for research is needed—above all, from industry. The development of one or more major multi-disciplinary research centres, following the model of CITRIS, is necessary to attract private funding and bring together experts from different academic departments and industry in a more integrated, multi-disciplinary research effort. We recommend that the Research Councils take the lead in initiating discussions with Government, universities and industry with a view to the prompt establishment of an initial centre in this country. (2.44)

8.5. Legitimate security researchers are at risk of being criminalised as a result of the recent amendments to the Computer Misuse Act 1990. We welcome the Minister's assurance that guidance on this point will appear later in the summer, but urge the Crown Prosecution Service to publish this guidance as soon as possible, so as to avoid undermining such research in the interim. (2.45)

The network

8.6. We see no prospect of a fundamental redesign of the Internet in the foreseeable future. At the same time, we believe that research into alternative network architectures is vital to inform the incremental improvements to the existing network that will be necessary in the coming years. We recommend that the Research Councils continue to give such fundamental research priority. (3.8)

8.7. The current emphasis of Government and policy-makers upon end-user responsibility for security bears little relation either to the capabilities of many individuals or to the changing nature of the technology and the risk. It

is time for Government to develop a more holistic understanding of the distributed responsibility for personal Internet security. This may well require reduced adherence to the "end-to-end principle", in such a way as to reflect the reality of the mass market in Internet services. (3.34)

8.8. The current assumption that end-users should be responsible for security is inefficient and unrealistic. We therefore urge the Government and Ofcom to engage with the network operators and Internet Service Providers to develop higher and more uniform standards of security within the industry. In particular we recommend the development of a BSI-approved kite mark for secure Internet services. We further recommend that this voluntary approach should be reinforced by an undertaking that in the longer term an obligation will be placed upon ISPs to provide a good standard of security as part of their regulated service. (3.67)

8.9. We recommend that ISPs should be encouraged as part of the kite mark scheme to monitor and detect "bad" outgoing traffic from their customers. (3.68)

8.10. We recommend that the "mere conduit" immunity should be removed once ISPs have detected or been notified of the fact that machines on their network are sending out spam or infected code. This would give third parties harmed by infected machines the opportunity to recover damages from the ISP responsible. However, in order not to discourage ISPs from monitoring outgoing traffic proactively, they should enjoy a time-limited immunity when they have themselves detected the problem. (3.69)

8.11. The uncertainty over the regulatory framework for VoIP providers, particularly with regard to emergency services, is impeding this emerging industry. We see no benefit in obliging VoIP providers to comply with a regulatory framework shaped with copper-based telephony in mind. We recommend instead that VoIP providers be encouraged to provide a 999 service on a "best efforts" basis reflecting the reality of Internet traffic, provided that they also make clear to customers the limitations of their service and the possibility that it may not always work when it is needed. (3.70)

Appliances and applications

8.12. The IT industry has not historically made security a priority. This is gradually changing—but more radical and rapid change is needed if the industry is to keep pace with the ingenuity of criminals and avoid a disastrous loss of confidence in the Internet. The major companies, particularly the software vendors, must now make the development of more secure technologies their top design priority. We urge the industry, through self-regulation and codes of best practice, to demonstrate its commitment to this principle. (4.38)

8.13. In particular, we urge the industry to endorse the following as best practice:

- Increasing the provision of security advice to users when first booting up PCs or launching applications;
- Automatic downloading of security updates upon first connecting machines to the Internet;

- Ensuring that default security settings are as high as practicable, even if functionality is restricted while users are still learning about the risks they face; and
- An industry-wide code of practice on the use of clear and simple language in security messages. (4.39)

8.14. However, efforts to promote best practice are hampered by the current lack of commercial incentives for the industry to make products secure: companies are all too easily able to dump risks onto consumers through licensing agreements, so avoiding paying the costs of insecurity. This must change. (4.40)

8.15. We therefore recommend that the Government explore, at European level, the introduction of the principle of vendor liability within the IT industry. In the short term we recommend that such liability should be imposed on vendors (that is, software and hardware manufacturers), notwithstanding end user licensing agreements, in circumstances where negligence can be demonstrated. In the longer term, as the industry matures, a comprehensive framework of vendor liability and consumer protection should be introduced. (4.41)

Using the Internet: businesses

8.16. The steps currently being taken by many businesses trading over the Internet to protect their customer's personal information are inadequate. The refusal of the financial services sector in particular to accept responsibility for the security of personal information is disturbing, and is compounded by apparent indifference at Government level. Governments and legislators are not in position to prescribe the security precautions that should be taken; however, they do have a responsibility to ensure that the right incentives are in place to persuade businesses to take the necessary steps to act proportionately to protect personal data. (5.53)

8.17. We therefore recommend that the Government introduce legislation, consistent with the principles enshrined in common law and, with regard to cheques, in the Bills of Exchange Act 1882, to establish the principle that banks should be held liable for losses incurred as a result of electronic fraud. (5.54)

8.18. We further believe that a data security breach notification law would be among the most important advances that the United Kingdom could make in promoting personal Internet security. We recommend that the Government, without waiting for action at European Commission level, accept the principle of such a law, and begin consultation on its scope as a matter of urgency. (5.55)

8.19. We recommend that a data security breach notification law should incorporate the following key elements:

- Workable definitions of data security breaches, covering both a threshold for the sensitivity of the data lost, and criteria for the accessibility of that data;
- A mandatory and uniform central reporting system;

- Clear rules on form and content of notification letters, which must state clearly the nature of the breach and provide advice on the steps that individuals should take to deal with it. (5.56)

8.20. We further recommend that the Government examine as a matter of urgency the effectiveness of the Information Commissioner's Office in enforcing good standards of data protection across the business community. The Commissioner is currently handicapped in his work by lack of resources; a cumbersome "two strike" enforcement process; and inadequate penalties upon conviction. The Government have expressed readiness to address the question of penalties for one type of offence; we recommend that they reconsider the tariffs for the whole of the data protection regime, while also addressing resources and enforcement procedures as well. These should include the power to conduct random audits of the security measures in place in businesses and other organisations holding personal data. (5.57)

Using the Internet: the individual

8.21. The Government-sponsored Get Safe Online website already provides useful information and practical advice to Internet users, but its impact is undermined by the multiplication of other overlapping websites. We recommend that the Government provide more explicit high-level political support to the Get Safe Online initiative and make every effort to recruit additional private sector sponsors. If necessary, the site should be re-launched as a single Internet security "portal", providing access not only to the site itself but acting as a focus and entry-point for other related projects. (6.46)

8.22. We agree with the Minister that there needs to be a "step change" in the way the regulator Ofcom approaches its duties in relation to media literacy. We recommend that Ofcom not only co-sponsor the Get Safe Online project, but that it take on responsibility for securing support from the communications industry for the initiative. (6.47)

8.23. We further recommend that, in addition to the new kite mark for content control software, Ofcom work with the industry partners and the British Standards Institute to develop additional kite marks for security software and social networking sites; and that it continue to keep under review possible areas where codes of best practice, backed up by kite marks, might be appropriate. (6.48)

8.24. We recommend that the Department for Children, Schools and Families, in recognition of its revised remit, establish a project, involving a wide range of partners, to identify and promote new ways to educate the adult population, in particular parents, in online security and safety. (6.49)

Policing the Internet

8.25. We recommend that the Government introduce amendments to the criminal law, explicitly to criminalise the sale or purchase of the services of a botnet, regardless of the use to which it is put. (7.74)

8.26. We recommend that the Government, in partnership with the Association of Chief Police Officers and the Serious Organised Crime Agency, develop a unified, web-based reporting system for e-crime. The public face of this system should be a website designed to facilitate public and business

reporting of incidents. The back-end software should have the capacity to collect and collate reports of e-crime, identify patterns, and generate data on the incidence of criminality. The website could also serve as a portal to other more specialised sites, for instance on online child abuse or identity theft. It would be an invaluable source of information for both law enforcement and researchers. (7.75)

8.27. As a corollary to the development of an online reporting system, we recommend that the Government review as a matter of urgency their decision to require online frauds to be reported to the banks in the first instance. We believe that this decision will undermine public trust in both the police and the Internet. It is essential that victims of e-crime should be able to lodge a police report and have some formal acknowledgement of the fact of a crime having been committed in exchange. We see no reason why such reports should not be made online, processed and forwarded to the banks automatically. (7.76)

8.28. If these recommendations are to be acted upon, the police service will need to devote more resources to e-crime. We acknowledge the good work undertaken by SOCA and on behalf of ACPO, but within the police skills and forensic capability still vary from force to force. While it is vital to raise police skills across the board, rather than just those of specialists, "mainstreaming" is only part of the answer. We therefore recommend the establishment of a network of computer forensic laboratories, under the aegis of the proposed ACPO national e-crime unit, but with significant central funding. (7.77)

8.29. We further urge the Home Office, without delay, to provide the necessary funds to kick-start the establishment of the Police Central ecrime Unit, without waiting for the private sector to come forward with funding. It is time for the Government to demonstrate their good faith and their commitment to fighting e-crime. (7.78)

8.30. These recommendations will all cost money. But e-crime is expanding rapidly: the choice is either to intervene now to make the necessary investment, and perhaps to keep the threat to the Internet under control, or to let it grow unchecked, and risk an economically disastrous, long-term loss of public confidence in the Internet as a means of communication for business and Government alike. (7.79)

8.31. We urge the Government to fulfil its commitment to ratify the Council of Europe CyberCrime Convention at the earliest possible opportunity. At the same time, in order to ensure that the United Kingdom fulfils the spirit as well as the letter of Article 25 of the Convention, we recommend that the Government review the procedures for offering mutual legal assistance in response to requests for help from other countries in investigating or prosecuting e-crime. (7.80)

8.32. Finally, we recommend that the Government take steps to raise the level of understanding of the Internet and e-crime across the court system. In particular:

- In the context of the prevalence of identity theft and online card fraud, we urge the Government to issue new guidance to the courts, including magistrates' courts, on the reliability of unsupported credit card evidence as an indicator of guilt;

- We recommend that the Government review the availability to the courts of independent specialist advice in cases of Internet-related crime;
- We believe that the sentence should fit the crime. The nature of e-crime is such that mostly (but not exclusively) small crimes are committed in very large numbers; they also generally involve a high level of intrusion into personal life. Sentencing guidelines should be reviewed in recognition of these realities. (7.81)

APPENDIX 1: MEMBERS AND DECLARATIONS OF INTEREST

Members:

Lord Broers (Chairman)
† Earl of Erroll
† Lord Harris of Haringey
† Baroness Hilton of Eggardon
Lord Howie of Troon
† Lord Mitchell
Lord O'Neill of Clackmannan
Lord Patel
Lord Paul
Baroness Sharp of Guildford
Lord Sutherland of Houndwood
† Lord Young of Graffham

† Co-opted Members

Declared Interests:

Lord Broers
Main Board Member, Vodafone

Earl of Erroll
Member, Nominet Policy Advisory Board
Member Information Systems Security Association Board
President, e-Business Regulatory Alliance

Lord Harris of Haringey
Member, Metropolitan Police Authority
Toby Harris Associates is doing business with The Anite Group, and Unisys Limited

Baroness Hilton of Eggardon
None

Lord Howie of Troon
None

Lord Mitchell
Chairman, eLearning Foundation
Shareholder, Syscap Holdings Ltd (a private company), an IT services provider
Shareholder, Apple Inc

Lord O'Neill of Clackmannan
None

Lord Patel
None

Lord Paul
None

Baroness Sharp of Guildford
None

Lord Sutherland of Houndwood

None

Lord Young of Graffham

Chairman and Shareholder, Pixology Plc, Spectra Interactive Plc and Eurotel Plc.

APPENDIX 2: WITNESSES

The following witnesses gave evidence; those marked with an * gave oral evidence:

* Professor Ross Anderson

AOL

Apache

APACS

* Ms Sandra Quinn
* Mr Colin Whittaker

British Computer Society

BT Group

Mr Duncan Campbell

Child Exploitation and Online Protection Centre

* Mr Jim Gamble

Ms Sharon Girling

Children's Charities' Coalition on Internet Safety

* Mr John Carr

Confederation of British Industry

* Mr Jeremy Beale

* Mr Alan Cox

Department of Trade and Industry

* Rt Hon Margaret Hodge MP
* Mr David Hendon
* Mr Geoffrey Smith

East Midlands Broadband Consortium

eBay

* Mr Gareth Griffith
* Mr Alasdair McGowan

EURIM

European Commission, Directorate-General for Information Society and Media

* Mr Achim Klabunde
* Mr Andrea Servida
* Mr Merijn Schik
* Ms Margareta Traung
* Ms Zinaida Yudina

* Mr Anthony Bisch
* Ms Valerie Gayraud
* Mr Rogier Holla
* Commissioner Viviane Reding

Federation of Small Businesses

Financial Services Authority
* Mr Philip Robinson
* Mr Rob Gruppetta

Mr Mike Forster

Professor Steven Furnell & Dr Andy Phippen

* Professor Mark Handley

Hewlett Packard

Home Office
* Mr Vernon Coaker MP
* Mr Tim Wright
* Mr Stephen Webb

Mr Nick Hubbard

Ilkley Computer Club

Information Commissioner's Office
* Mr Phil Jones

Institute for the Management of Information Systems

Institute of Information Security Professionals

Internet Services Providers' Association
* Ms Camille de Stempel
* Mr Matthew Henton
* Mr James Blessing

Internet Telephony Services Providers' Association
* Mr Kim Thesiger

* Mr Adam Laurie

Law Society
* Mr Nicholas Bohm

London Internet Exchange
* Mr Malcolm Hutty
* Mr John Souter

MessageLabs
* Mr Mark Sunner

* Mr Paul Wood

Metropolitan Police

* Commander Sue Wilkinson

Microsoft

* Mr Jerry Fishenden

* Mr Matt Lambert

National Computing Centre

National Education Network

Ofcom

* Mr Tim Suter

* Mr Ben Willis

* Mr Jeremy Olivier

Office of Fair Trading

* Mr Mike Haley

Mr Paul O'Nolan

Orange UK

PAOGA

PayPal

* Mr Michael Barrett

Ready Technology

Research Councils UK

Royal Academy of Engineering

Royal Bank of Scotland

* Mr Matthew Pemble

* Mr Bruce Schneier

SecureTrading

Serious Organised Crime Agency

* Mr Bill Hughes

* Ms Sharon Lemon

Ms Margaret Smith

Society for Computers and Law

* Professor Ian Walden

Symantec

* Mr Roy Isbell

* Mr Ilias Chantzos

THUS

Mr Brian Tompsett

UKERNA

* Dr Andrew Cormack

VISA

* Ms Sandra Alzetta

* Mr Robert Littas

Mr Paul Winstone

* Professor Jonathan Zittrain

The following evidence has not been printed but is available for inspection at the Parliamentary Archive (020 7219 5314):

Mr Brian Catt

Edentity

Terence Grange, ACPO

Institution of Engineering and Technology

APPENDIX 3: CALL FOR EVIDENCE

The inquiry invites 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.

In particular, the Committee invites evidence on the following questions:

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?

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?
- 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?
- What factors may prevent 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?
- Who should be responsible for ensuring effective protection from current and emerging threats?
- What is the standing of UK research in this area?

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

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?

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

APPENDIX 4: SEMINAR HELD AT THE INSTITUTION OF ENGINEERING AND TECHNOLOGY, SAVOY PLACE, LONDON

28 November 2006

Members of the Sub-Committee present were Lord Broers (Chairman), Lord Mitchell, Lord O'Neill of Clackmannan, Lord Patel, Baroness Sharp of Guildford, Lord Sutherland of Houndwood, Lord Young of Graffham, Dr Richard Clayton (Specialist Adviser), Christopher Johnson (Clerk) and Cathleen Schulte (Committee Specialist).

Participants were Maria Burroughs (DTI), Professor Brian Collins (Professor of Information Systems, Cranfield University), Cordella Dawson (Home Office), Robert Gruppetta (FSA), Malcolm Hutty (Head of Public Affairs, LINX), Matt Lambert (Government Affairs Director, Microsoft), Adam Laurie (The Bunker), Ben Laurie (The Bunker), Sharon Lemon (Deputy Director of e-crime, SOCA), Detective Chief Inspector Charlie McMurdie (Metropolitan Police), Philip Virgo (EURIM), Tim Wright (Home Office).

Personal Internet security – key themes (Dr Richard Clayton)

Dr Clayton gave an overview of the subject-matter for the inquiry. There was a general perception that people were unsafe on the Internet, and that things were getting worse. Whose fault was this? There was a long list of potential candidates who could take a share of responsibility:

- Operating system vendors were shipping products before they were secure;
- End-users weren't patching their systems to fix security holes;
- Application programmers were paying no attention to security;
- Businesses running applications weren't patching their systems to keep them up-to-date;
- Retailers were selling un-patched systems and not giving users enough support in setting up a complex product;
- ISPs were letting bad traffic reach end-user machines and not insisting their customers were secure;
- Hardware manufacturers weren't making routers and modems "secure by default";
- Networks weren't providing secure DNS (name services) or BGP (routing);
- Companies were marketing VoIP as if was just as reliable as conventional telephony;
- Regulators weren't setting minimum security standards or trying to fix market failures;
- Criminals were doing bad things;
- The police weren't bothering to catch them;
- Legislators weren't enacting suitable laws;

- The Government weren't making sure that overseas crooks were dealt with;
- The Information Commissioner wasn't dealing with spam;
- End-users were going to unsuitable websites and downloading pirated material;
- Educators weren't teaching "media literacy" effectively enough;
- Banks weren't giving customers security devices;
- Credit card companies were dumping their risks onto merchants;
- Web businesses weren't keeping customer records secure;
- And perhaps it was all state-sponsored InfoWar!

In reality most of the people in the areas listed above were doing their best and improving their own little part of the puzzle. But it was not a simple problem with a simple solution. The important thing was to better align incentives so that things began to improve rather than continuing to get worse.

The nature and scale of the threat to private individuals (Mark Harris, Global Director, SophosLabs)

Mr Harris noted that viruses now tended not to replicate widely—of the over 3,000 new viruses reported each month, the majority were Trojans, installed on PCs via spam, which installed other unwanted software, but did not replicate. They were designed to make money, not to vandalise the Internet, and were targeted at un-patched machines. Machines which were patched up to date were unlikely to be infected.

Users tended to look on computers as white goods—security was the last thing on their mind. They were completely unaware of the risks of clicking on pop-ups or hyperlinks. In some cases even unopened emails could now infect machines if they were being previewed.

In answer to questions, Mr Harris said the IT security business was working round the clock to keep up with the changing threats. However, there was still uncertainty as to the policing response to cyber-crime—there was no alert system in place for reporting fraudulent websites etc.

Public education and engagement (Professor Bill Dutton, Director, Oxford Internet Institute)

Professor Dutton described the Oxford Internet surveys, based on interviews with around 2,000 people. These revealed that home was the key location for Internet use; people learnt about the Internet from friends and family rather than through formal teaching or documentation. Most users, even experienced users, had no experience of writing programmes or creating web pages. Nevertheless, people seemed to be coping somehow—not just individuals, but manufacturers and ISPs.

Regulation and legislation (Professor Ian Walden, Reader in Information and Communications Law, Queen Mary, University of London)

Professor Walden drew attention to the variety of criminal activity, from teenage hackers to organised crime. Large numbers were involved, and this created

challenges for the criminal justice system, which struggled to cope with large numbers of suspects.

There were essentially three kinds of criminal conduct on the Internet:

- Traditional crime, such as fraud, using computers as a tool (e.g. phishing), covered by existing criminal law;
- Content-related crime, where the content (e.g. child abuse images) was illegal. Traditionally the law differentiated between supplying and possessing content, but this was harder to sustain in the computing environment;
- Crimes against confidentiality and the integrity of computers—the Computer Misuse Act 1990 had recently been amended so as to cover denial of service attacks.

Legislation in recent years had tended to change and extend the way in which offences were investigated (online child abuse sometimes being used as a pretext) rather than creating new offences. In addition, the international dimension of cyber-crime had led to harmonisation of legal regimes at EU and Council of Europe levels. However, there was now a need to think about laws to promote security, rather than just penalising and investigating offences.

Policing the Internet (Detective Superintendent Russell Day, Metropolitan Police Specialist and Economic Crime Directorate)

DS Day, while drawing attention to the variety of criminal activities online, argued that there were few new crimes. The National e-Crime Coordination Unit was being developed as a centre of excellence in combating such crime.

Most of the Metropolitan Police's resources were currently being taken up by forensic work, analysis of hard drives etc—the resources available for investigating criminal networks such as botnets were very limited. Training was very resource-intensive—though the Met could call on some 150 special constables with IT skills to assist in particular investigations.

The security of operating systems (Ed Gibson, Chief Security Officer, Microsoft UK)

Mr Gibson drew attention to Microsoft's responsibility to ensure that anyone logging onto the Internet using a Microsoft platform was as secure as possible. Thus the new Internet Explorer 7 included a phishing filter. However, human nature was such that people would inevitably visit unsuitable sites regardless.

All Microsoft products went through a cycle of security reviews, including a "final security review", conducted in the immediate run-up to launching a new product.

Internet service provision (John Souter, CEO, LINX)

Mr Souter noted that five companies supplied 75 percent of broadband customers: BT, NTL, AOL, Tiscali and Orange. But in addition there were hundreds of smaller companies, selling mainly on price. At the same time, there was no published evidence to show that any one ISP was more secure than any other.

Asked whether ISPs could block bad traffic, Mr Souter argued that they could not. It was difficult to identify bad traffic (e.g. when it was encrypted), and it was very mobile and variable, making it very hard to maintain up-to-date filters.

Commerce over the Internet (Nicholas Bohm, Law Society)

Security was about personal and commercial relationships. "Security" in the old sense—e.g. security for a loan—was a way to offer guarantees to particular creditors. But more security for one creditor might mean less for another. Typically in an online fraud there would be two innocent parties (say, a bank and a customer), and a fraudster in the middle. The two innocent parties would be left in dispute over meeting the cost—security was about striking a balance between them.

PCs were not secure. Instead responsibility for security was shared out via contracts so as to manage the risk. With credit cards customers were in a good position—the banks met the cost of fraud in customer-not-present transactions. But where such risks were passed onto merchants the situation was less favourable.

Customers could not be held liable if their bank honoured a cheque with a forged signature—however, this did not apply online. At the moment banks' security protocols relied on shared secrets. This was no longer acceptable. The key was to create incentives to invest in improved security—this meant ensuring that risks fell where it was most expedient for the whole community that they should fall.

New technologies and emerging threats (Professor Ross Anderson, Cambridge University)

Professor Anderson outlined the subject of "security economics". The traditional view of info-security was that failures were down to a lack of technical features such as firewalls. However, in recent years it had become clear that systems were insecure whenever those who could fix them had no incentive to do so. UK banks were less liable for fraud than US banks—but suffered more fraud as a result.

The economics of the IT business were such that competition to get to the top was fierce, sidelining security. Once a company had reached the top (as Microsoft had done), the situation was different, and increased security could be used to lock out competition.

Overall, we were spending more or less the right amount on security. But spending was skewed: big companies were spending too much, Government far too much, but small companies too little.

Discussion

Discussion initially focused on policing. Police forces were focused on local crime, not on the international co-ordination needed to combat cyber-crime. SOCA had a more outward focus, inheriting good relationships with international partners from the National High-Tech Crime Unit, and targeting both the countries from which cyber-crime mostly originated and the five main target countries. At the same time SOCA aimed to identify overlaps and gaps in the work of individual police forces.

There was a perception that "level 2" crime was being overlooked. This had in fact been the case even before the absorption of the NHTCU into SOCA, and law enforcement still had not got it right. There had to be confidence that when level 2 crime was reported it would be picked up, and at the moment this was not happening. However, the police were now working with APACS to develop a reporting system from banks to the police.

It was argued that there were discrepancies between the amounts spent on law enforcement, the relatively small actual losses, and the huge amounts spent by individual users on IT security. Attempts to change behaviours were hampered by

weak incentives, leading to players pushing risk up or down the chain. At the same time political moves to create specialised units to combat cyber-crime might be less productive than less visible efforts to raise skills across the board.

A particular problem was the distortion produced by child abuse cases—the pressure to devote resources to investigating child abuse was irresistible, and could compromise other policing priorities. Operation Ore had brought law enforcement services to their knees.

Discussion then turned to data protection and the security breach notification laws in some US states. It was argued that a security breach notification law would be a potent incentive to improve security. In a recent case in the UK, a major supermarket, one of whose ATMs had been compromised by a "skimmer", refused to co-operate in contacting customers who had used the ATM, and police had had to put an advertisement in the local paper to reach them. In the US the supermarket would have been obliged to write to every customer, in effect admitting negligence and warning them to check bank statements. This provided protection for customers who were subsequently victims of fraud and who could use such notification to help prove this to their bank.

In contrast, the position in the UK was that companies whose security had been compromised were under no obligation to disclose the fact, and were in fact advised to keep quiet and wait to be sued. A security breach notification law in the UK would be a major help to law enforcement, not least in helping to identify the scale of the problem. It should not be limited to telecommunications companies, but should be tied to data protection, covering all institutions holding personal data.

Finally discussion focused on emerging technologies. Increasing numbers of appliances incorporated computers, and relied on the Internet to communicate. Thus the Internet could be used to compromise an ever-widening range of technologies. For instance, information collected from airline websites could be used to compromise ID cards and e-passports. Furthermore society as a whole was increasingly reliant on the Internet to support critical services, such as hospitals. The time was rapidly approaching in which a failure of the Internet would lead directly to deaths. There was an issue over whether reliance on the Internet for critical services was prudent.

APPENDIX 5: VISIT TO THE UNITED STATES

Members of the Sub-Committee taking part in the visit were Lord Broers (Chairman), Lord Harris of Haringey, Baroness Hilton of Eggardon, Lord Howie of Troon, Lord Mitchell, Dr Richard Clayton (Specialist Adviser) and Christopher Johnson (Clerk).

Washington DC, Monday 5 March

Federal Trade Commission

The Committee was welcomed by Hugh Stevenson, Associate Director for International Consumer Protection, and colleagues Katy Ratté, Nat Wood and Jennifer Leach. The FTC had around 1,100 staff, including some 300 in the Bureau of Consumer Protection.

It was noted that the US had no comprehensive, over-arching data protection or privacy legislation. There was however a requirement for all companies to put in place reasonable processes to assure security of personal data—this approach was preferred to the setting of detailed technical requirements. The assessment of "reasonableness" was flexible, depending on the size of the company, the sensitivity of data, and so on.

The role of the FTC was to monitor proactively the security measures put in place by financial institutions (including all companies providing financial services, but excluding the major national banks, which were regulated by the Federal Reserve), and to investigate specific complaints with regard to other companies. The FTC had discretion to decide which complaints to pursue, based on the seriousness of the issues raised. If companies did not have "reasonable" processes in place, the FTC could either make an order requiring improvements, or could seek civil penalties. The FTC had yet to enter into litigation on the scope of reasonableness, but voluntary enforcement orders had been entered into by a number of companies, including Microsoft, with regard to its Passport programme.

The FTC received over 450,000 complaints of identity theft each year, and surveys put the total number of cases at 8-10 million a year in the US. Work to disaggregate ID theft from simple card fraud was ongoing. The FTC now required a police report to be filed, which in turn triggered investigation by financial institutions. However, the numbers of cases investigated were very small.

Data breach notification laws in over 30 states had had a marked impact, driving many investigations, notably the Choicepoint case, which resulted in the company paying $10 million in civil penalties and $5 million in redress to customers. However, the inconsistency between state laws created some difficulties, and Congress was now looking at a federal data breach notification law.

On spam, the "Can-Spam" Act had provided for suits by private individuals or companies, and Microsoft and other companies had brought cases; the FTC itself had brought around 100 cases. The approach was normally to focus on what spam was advertising, and thus who profited from it, rather than seeking to identify the source of spam emails themselves.

State Department

The Committee was welcomed by Mr Richard C Beaird, Senior Deputy Co-ordinator for International Communications & Information Policy. The role of the

State Department was to co-ordinate international initiatives on cybersecurity, such as the "Information Society Dialogue" with the European Commission. The State Department also advocated the Council of Europe's Convention on Cybercrime, which the US had now ratified.

Co-ordinated action was difficult, given the asymmetry between legal systems around the world. However, cybersecurity was an increasingly high priority internationally. Bodies such as the OECD, the International Telecommunications Union (ITU) and Asia-Pacific Economic Cooperation (APEC), were engaging with issues such as spam and malware, and with capacity building designed to help less developed countries confront these problems. The UK was a strong partner in such international initiatives.

The top priority was to develop laws within domestic legislation that put people in jail. In so doing, technical measures to help identify sources of, for example, spam, would be valuable.

On mutual legal assistance, which figured in the Council of Europe Convention, the US participated actively in the work of the first UN Committee on police co-operation. However, in pursuing cases internationally there had to be a balance between pursuing criminality and protecting freedom of speech.

Lunch

The Committee attended a lunch hosted by the Deputy Head of Mission, Alan Charlton. Guests included Stephen Balkam, CEO of the Internet Content Rating Association; Peter Fonash, Department of Homeland Security; Liesyl Franz, IT American Association; Michael R Nelson, Internet Society; and Andy Purdy, President of DRA Enterprises, Inc.

Team Cymru

The Committee spoke to Jerry Martin, Research Fellow, who said that Team Cymru had begun as a think-tank, before being incorporated in 2005. It now employed a network of researchers dedicated to supporting the Internet community in maintaining security; it was funded by grants and a small number of commercial contracts, but was non-profit making.

On one day, the preceding Saturday, Mr Martin had detected over 7,000 malicious URLs, over half of these hosted in China. These were identified through a database of malicious code samples, currently being added to at an average rate of 6,200 a day. Of these samples around 28 percent were typically being identified by anti-virus software; the information was then made available to Symantec, and by the end of the month the average detection rate increased to 70 percent.

If all the examples of malicious code were to be reported to the police, they would be overwhelmed. There were legal process in place, both nationally and internationally, to investigate them—the problem was one of time and resources. The FBI cybercrime division employed relatively few people. Well qualified staff soon found they could earn a lot more in the private sector, leading to large numbers of vacancies in government agencies.

Mr Martin then illustrated the working of the underground economy in stolen identities, credit card details etc., using examples from Internet Relay Chat (IRC) rooms.

The official reported loss to banks of $2.7 billion a year was under-reported—there was an incentive in the financial community to down-play the problem. Education

of consumers was not really a solution—you would never be able to stop people from clicking on links to corrupt websites. The key for banks and others was:

- To introduce two-factor authentication;
- To ensure that companies were familiar with all their address space, rather than bolting on new areas, for instance when acquiring new subsidiaries;
- To be more demanding of software manufacturers.

Progress and Freedom Foundation

The Committee met Tom Lenard, Senior Vice President for Research, and colleagues. Mr Lenard approached the issues as an economist, recognising the huge benefits derived from the Internet, and asking whether there was market failure or harm to consumers, and whether government action was needed to remedy any such problems.

The best available statistics (e.g. Javelin and the Bureau of Justice) indicated that levels of identity theft had on most measures been in decline in the last three years, and that the overall problem was smaller than normally represented. On the other hand, the retention of information by companies was what often allowed them to identify anomalous transactions so quickly, and so benefited consumers. Mr Lenard accepted that the reliability of the available data was open to question, but cautioned against assuming that a lack of data meant an increasing problem.

On the security of operating systems, companies such as Microsoft and Apple were spending a huge amount on security, and there was no evidence that new incentives were needed. Governments were not well placed to decide levels of security, encryption and so on. The approach of the FTC, requiring reasonable standards of security, was a better approach. In addition, the FTC had launched major litigation, for instance against Choicepoint. These had created a significant deterrent to private sector companies from persisting with poor security practices. However, Government was almost certainly not spending enough on security, and this would be an appropriate area to regulate.

On spam, the Can-Spam Act had had no effect on levels of spam. Intervention on spam was technically difficult, but the Internet was young and evolving new technical solutions. Government intervention had not helped.

Washington DC, Tuesday 6 March

Department of Justice

The Committee met John Lynch, Deputy Chief, Computer Crime and Intellectual Property, and colleagues Chris Painter and Betty-Ellen Shave. The Department of Justice itself had around 40 attorneys working on cybercrime and intellectual property. It also supported a network of 200 federal prosecutors around the US specialising in high-tech crime, working closely with the FBI and local law enforcement.

The FBI now had cybercrime as its number three priority, after international terrorism and espionage. At the same time the US, like all countries, lacked resources to deal with cybercrime; in particular many local police forces had difficulty conducting computer forensics. These problems were compounded by the loss of qualified investigators to the private sector.

Moreover, there were no unified definitions or reporting systems for cybercrime or identity theft, and statutes varied from state to state. Victims who reported small cybercrimes to local police, who lacked expertise, were unlikely to get anywhere. This created particular problems in investigating small crimes—say, under $1,000—which would not justify federal prosecutions. However, if victims reported small crimes to the "IC3" (Internet Crime Complaint Center), the FBI would "triage" them, which meant there was a chance of linking up many small cases so as to turn them into larger, potentially federal, cases.

The President had asked for a report on identity theft, and the DoJ was co-operating with the FTC, FBI and Secret Service in considering the issues. The report was likely to appear in the next two or three months. The FTC was pressing for uniform reporting procedures for ID theft, and this might well figure in the report.

Reporting rates were low, and many crimes were swallowed up by the credit card companies. The general feeling was that law enforcement was not keeping up with cybercrime, and this appeared to be having a damaging effect on the growth of e-commerce. While there were prosecutions, only a small percentage of crimes ended up in court. Whereas ten years ago cybercrime was the domain of experts, now the general criminal, with no special abilities, could commit crimes online.

The UK had been prominent in multi-lateral actions, and was probably ahead of the US in protecting critical IT infrastructure. However, whereas the US had ratified the Council of Europe convention, it was still urging other states (including the UK) to ratify. The creation of a 24/7 emergency network meant that law enforcement officers from around 50 countries could at any time request assistance from US experts; there was no guarantee that requests would be granted, but they would be considered without delay.

As for the Mutual Legal Assistance and hot pursuit provisions of the convention, the US was slower than some other countries in closing down rogue websites. In particular, the 1st Amendment, guaranteeing freedom of speech, dictated a cautious approach. At the same time, law enforcement had developed good relations with ISPs, who could close sites that breached their terms and conditions.

The key recommendations were, first, for the UK to ratify the Council of Europe convention, and, second, to increase resources for law enforcement.

Verisign

The Committee was welcomed by Shane Tews, Senior Washington Representative, who outlined the role of Verisign. The company ran two of the thirteen top-level roots (the "A" and "J" roots) of the Internet. It also supported the database registry for the .com and .net domains. It employed just under 4,000 people globally, and maintained servers around the world. This allowed regional resolution of "bad traffic"—in effect, bad traffic emanating from, say, Russia, could be sunk in a regional "gravity well", rather than slowing down the Internet as a whole.

Verisign could not specifically identify the IP addresses of the originators of bad traffic, such as spoof emails, but it could identify the IP addresses of servers—in effect, the wholesalers—and engage with them.

Personal Internet security could not be separated from the integrity of the infrastructure as a whole. The volume of bad traffic, much of it targeted ostensibly

at individual users, affected the entire network. The originators were variously organised criminals, terrorists and rogue states. Secure, government-run financial networks now handled around $3 trillion of traffic every day. These networks did not interact directly with the public Internet, but such transactions would not be possible if public sites, such as the New York Stock Exchange, or the Bank of England, were not operating. The Internet had to be viewed holistically—the costs of insecurity were potentially huge.

The level of bad traffic—for instance, the DOS attack on the .uk root server in February 2007—was now peaking at 170 times the basic level of Internet traffic; by 2010 it was likely to be 500 times the basic level. Massive over-capacity and redundancy was needed to allow enough headroom in the network to accommodate such traffic. Verisign alone was now able to handle four trillion resolutions per day on its section of the network, some eight times the normal current volume across the entire network.

More broadly, Verisign was a private sector company, in effect performing a public service in maintaining the network. The Internet had not been designed to support the current level of financial traffic—it had just happened that way. Authentication of websites was a service offered by Verisign, and the process of securing authentication for major companies such as Microsoft was very thorough. But in the longer term the question would arise of whether, and if so when, individuals would be prepared to pay for authentication of Internet-based services, such as email, which were currently free.

Internationally, certain states in eastern Europe and Asia were turning a blind eye to organised crime operating via the Internet from within their borders. Although the Council of Europe convention was a huge step forward, it was essential to engage local authorities and agencies in combating this phenomenon.

California, Wednesday 7 March

University of California, Berkeley Center for Information Technology Research in the Interest of Society (CITRIS)

Introduction

The Committee was welcomed by Gary Baldwin, Executive Director of CITRIS. CITRIS had been established some six years ago, on the initiative of former Governor Gray Davis. It was an independent research centre, reporting directly to the President of the University. A small amount of money, sufficient to cover operating costs, came from the State of California. Funding for research came from partner organisations in industry and federal government (such as the National Science Foundation). Of the staff, over half were from electrical engineering and computing; engineering, other sciences, and social sciences, made up the remainder.

Shankar Sastry

Professor Sastry said that the point of CITRIS was to bring together technologists with experts in the social science field to develop a co-ordinated approach to cybersecurity research. CITRIS itself was an umbrella organisation, which sheltered a number of different research priorities.

Many companies had made pledges (typically $1.5 million a year) to support research, making good these pledges by buying membership in particular research

centres, such as TRUST, rather than by contributing to a central pot. These centres, with 5-10 researchers, were fluid, normally breaking up and re-forming over a five-year cycle.

CITRIS took the view that new technologies should be put in the public domain. The results of research were published and made available by means of free licensing agreements (in other words, not open source). Industry partners had to leave their intellectual property behind when engaging in CITRIS research projects; however, they were free to make use of the results of these projects to develop new products with their own IP.

TRUST (the Team for Research in Ubiquitous Secure Technology) was one of the research centres, and organised its work on three planes: component technologies; social challenges; and the "integrative" layer between them. Issues investigated included phishing and ID theft, with particular emphasis on the collection of reliable data. Statistics were currently based largely on self-selected surveys, and banks still regarded ID theft as marginal. However, the growth rate was exponential, and in recent years, through a "Chief Security Officer Forum", a number of companies, such as Wells Fargo, Bank of America and Schwab, were taking the issue more seriously.

TRUST had established a test-bed for network defence systems, in which different kinds of attack could be simulated. Technological transfer included anti-phishing products such as SpoofGuard, PwdHash and SpyBlock.

CITRIS research centres were constantly looking for international partners, and a symposium was being organised in London in July. The question was raised as to whether British universities should establish a similar research centre, in collaboration with industry.

Vern Paxson

Dr Paxson outlined his research detecting and collating network intrusions. The goal of information security policy was risk management. False positives and false negatives were the Achilles' heel of all intrusion detection, and, scaled up, undermined assessment of the risks. His laboratory focused on real Internet traffic, rather than simulations, and in so doing detected from the high 100s to low 1,000s of attacks each day.

Analysis of packets as they passed required highly specialised hardware, which ISPs did not have access to. This meant that ISPs were simply not in a position to filter Internet traffic and achieve an adequate level of false positives and false negatives.

Mass attacks were targeted at large parts of the network at once—they were not targeted. Botnets were the key problem—the cost of renting a compromised platform for spamming was currently just 3-7 cents a week. The total number of compromised machines was unknown—a guess would be around five percent, or 10-20 million. There was no evidence to suggest that some countries were significantly worse than others.

The research raised legal problems. One was the restriction on wire tapping. More fundamental was the fact that a platform that allowed incoming traffic but barred outbound traffic could be easily finger-printed by the "bad guys"; but to allow outbound traffic risked infecting other platforms, and could make the centre liable for negligence.

Chris Hoofnagle

Mr Hoofnagle noted that the US now had 34 state laws on security breach notification, and a federal law covering the Veterans' Agency. Within these there were various definitions of what constituted a security breach, with the California law the most demanding. In contrast, some states required evidence of potential for harm. There was now pressure for a federal law on security breach notification, which was likely by the end of 2007. It appeared that the FTC would be responsible for implementation.

The Center had collected 206 examples of notification letters, and was coding them under various criteria. However, the collection was by no means complete—only a few states (around five) required centralised notification to a specified regulator. These also required the use of standardised forms, which were crucial to providing good data.

There was some evidence that the media had lost interest in security breach notification, reducing the incentive to raise security levels to avoid tarnishing company image. However, a central reporting system, bringing together information on company performance in a generally accessible form, would help counteract this.

Data on ID theft were also very poor. The Javelin survey estimated 8 million cases in 2006, but relied on telephone surveys. Online polling put the figure at nearer 15 million. Estimates of the damage ranged from $48-270 billion in 2003. Data were also lacking on "synthetic ID theft", where a stolen social security number was combined with a made-up name. Assertions that most ID theft was perpetrated by persons close to the victim (family members etc.) were based on very small samples.

Paul Schwartz

Professor Schwartz drew attention to the split in the US, as in most countries, between law enforcement and intelligence agencies. While there was good information on the former, little was known about the latter.

There were two levels of law: constitutional and statutory or regulatory. The main constitutional law derived from the Fourth Amendment, on the requirement for a warrant for searches and seizures, based on probable cause. Until 1967 there had been no privacy for telecommunications, but at that point the Supreme Court had established the requirement for a search warrant for tapping, on the basis of the individual's "reasonable expectation of privacy". This had since been curtailed by rulings that the Fourth Amendment did not apply either to information held by third parties (e.g. bank records) or to "non-content", such as lists of numbers dialled.

Modern communications meant that ever more information was being held by third parties, such as emails stored on servers. In addition, information is not communicated in real time (as telephone conversations were in 1967), with the result that the Fourth Amendment does not apply. The result was that there was little protection under the US Constitution.

Maryanne McCormick

Ms McCormick drew attention to the need for the technology companies that operate the network to lead in tackling the problems. A common complaint was that universities were not training enough graduates to support these companies,

and Science, Technology and Society Center was therefore developing an industry-backed security curriculum, with web-based modules covering such issues as risk management, policy and law.

Around 85 percent of the critical infrastructure was developed, owned and maintained by the private sector. The Center was exploring how decisions were taken by the companies involved, the roles of Chief Security Officers and Chief Privacy Officers, how they were qualified, what sorts of technologies they acquired, and how internal security policies were set. Security and privacy were not profit-generating, but drew on resources generated by other profit-making sectors. The Center was looking at how security breach notification laws impacted on decision-making in this area.

Finally, researchers were looking at the barriers, in particular the difficulty of accessing network traffic data. The US legal regime (e.g. the Stored Communications Act) was having a chilling effect on research.

Electronic Frontier Foundation

The Committee met Gwen Hinze, Daniel O'Brien, Seth Schoen and Lee Tien from the Electronic Frontier Foundation, a not-for-profit organisation founded in 1990, with 13,000 paying members, dedicated to representing innovators and supporting civil liberties for the consumer on the Internet.

The focus of the EFF was increasingly on litigation and education, rather than policy-making. The biggest case currently being undertaken was a class-action lawsuit against AT&T for their involvement in the National Security Agency's programme of wire-tapping communications. The EFF employed 12 attorneys, but also leveraged support from other organisations. Cases were taken on a pro bono basis.

There EFF had three positive recommendations: to focus on prosecuting real Internet crime; to explore possible changes to incentive structures to address market failures in the field of Internet security; to empower and educate users, rather than following the emerging trend to lock down devices.

On the last of these, the EFF was concerned by the increasing tendency to take control over their own systems away from users. While such control, exercised by, say, network operators, might be exercised from benign motives, it effectively imposed a software monopoly upon users, limiting innovation. At the same time, insecurities often resided within operating systems and applications themselves, so that the current focus on firewalls and anti-virus software was misplaced. The key was to empower and educate users to manage their own security intelligently, rather than to adopt a paternalistic approach which would only store up problems for the future.

There were many well-documented security problems that the market had not fixed. New incentives were therefore needed. Vendor liability risked encouraging companies to shift liability to users, by exerting ever more control over end users, and the EFF was therefore equivocal on the desirability of such a regime. It would also impact on innovation, open source software, small companies and so on. More research and analysis of new incentives was needed.

A significant percentage of computers had already been compromised by organised crime. However, botnets were not affecting end users directly, but were being used for spam and DOS attacks. As a result end users needed more information, not

less, so that they could evaluate the position more intelligently. They needed a reason to care.

Dinner

The Committee attended a dinner hosted by Martin Uden, the Consul General. The guests were Whit Diffie, CSO, Sun Microsystems, John Gilmore, Founder, Electronic Frontier Foundation, Jennifer Granick, Executive Director of the Stanford Center for Internet and Society, and John Steward, CSO, Cisco Systems.

California, Thursday 8 March

Silicon Valley Regional Computer Forensic Laboratory

The Committee was welcomed by Mr Chris Beeson, Director of the Laboratory, and then heard a presentation from Special Agent Shena Crowe of the FBI. She began by commenting on the availability of data. The FTC led on ID theft, and individuals were required to report theft to local police in the first instance. The FBI ran the Internet Crime Complaint Center (IC3), and individuals were encouraged to report offences to this site by other agencies and police, but the police report was the fundamental requirement. Reporting to IC3 was voluntary.

In 2006 complaints to IC3 reached 20,000 a month. Losses reported in 2005 were $183.12 million, with median losses of just $424. Over 62 percent of complaints related to online auctions.

Cybercrime was a maturing market. There was a lot of money to be made, and although there were some individual criminals organised crime led the way. Underneath this level there were many specialists in such areas as rootkits. Communications within the criminal world were conducted through IRC (Internet Relay Chat), P2P (Peer-to-Peer), and tor (The Onion Router). Typically first contacts would be made via IRC, and deals would then be made in other fora. Team Cymru and other volunteer groups played a critical part in monitoring this traffic—the FBI, as a Government agency, could not lawfully monitor or collect such data, whereas researchers were able to do so.

In terms of security, the key players were the industry itself, the Department for Homeland Security, FBI, IT Information Sharing and Analysis Centers (IT-ISAC, in which company security specialists shared best practice), and the Secret Service. Within the FBI the cybercrime division was established six years ago, and staff and resources had in recent years shifted from conventional criminal work to the top priorities of counter-intelligence, terrorism and cybercrime.

International action was difficult and often informal. Requests for help could be ignored or subject to barter. There were few reliable data on the main centres of organised cybercrime, though Russia and China were commonly cited as major sources.

Security breach notification laws had been beneficial in helping companies to normalise the issues. Rather than sweeping breaches under the carpet they were now more likely to assist investigations. However, the reality of investigations was that from an attack on a particular target, to tracking down the drones and the botnet, to reaching the source, could take months. Investigations were not operating in digital time. Ms Crowe then took the committee through the various stages of one particular investigation, which had taken about a year to complete.

ISPs were now beginning to sand-box infected computers used to send spam and so on. However, the reality was that criminal innovation was a step ahead of enforcement. In 2005 six major US companies experienced theft of personal identifying information, with insiders increasingly being implicated. These cases were all reported to the FBI by the companies concerned.

Mr Beeson then told the Committee that there were 14 Regional Computer Forensic Laboratories. The volume of data processed had increased from some 40 Tb in 2000 to over 1,400 Tb in 2005. Processing this volume of data required specialised laboratories, focusing solely on computer forensics. The RCFLs were set up in partnership with local law enforcement, who provided personnel. In return, the RCFL would provide forensic analysis, at no cost to the local police. Federal funding supports running costs, such as premises and equipment.

Mr Beeson then gave the Committee a short guided tour of the facility.

Apple

The Committee met Bud Tribble, Vice President, Software Technology, and Don Rosenberg, Senior Vice President and General Counsel. Dr Tribble noted that while in the 1980s no-one had anticipated the security issues associated with the Internet, security was now a top priority not just for Apple but for every other company in the industry. In 2000 Apple had replaced its existing operating system with a Unix-based system, which had been covered with a usable top layer to create a secure platform.

Security started with good design. Security had to be easy to use, or else people would not use it. Apple went out of its way not to ask users security questions, to which they would not know the answers. There was no simple fix for security, no "seat belt" for Internet users, but overall security continued to improve incrementally.

Asked about vendor liability, Dr Tribble argued that there were many causes for, say, a virus infection—the virus writer, the user who downloaded the virus, and so on. It was difficult to assign responsibility or liability. The key was to incentivise continuing innovation—it was not clear that vendor liability would create such an incentive.

However, by taking decisions away from users Apple was implicitly taking on more liability. The company took decisions which could prevent users from downloading and running material—indeed, on the iPhone it would not be possible to download any applications. People had protested, and Microsoft systems certainly allowed more freedom, but they also created more problems. Looking to the future, Apple was conducting research into the possibility of including a sand-box in which applications could be run securely, but this was two or three years away.

Ultimately the market would decide. The problem was that at present there was not enough transparency or information within the market to enable consumers to take such decisions. Security and usability had to be balanced. There were technical fixes to security issues—PGP encryption, to address the traceability of email, had been around for more than 10 years—but they were not usable for general users.

Spam was a major issue. The reason there was so much spam was that there was an economic incentive to create it. In addition, Can-Spam had been ineffective—it was not enforceable, and many of the spammers were operating outside the law

anyway. Apple used a filtering technology to filter out spam. Although there were reports of Macs in botnets, they appeared to be very rare, and the evidence was largely based on hearsay. The company had yet to see a Mac botnet. The most fruitful avenues for dealing with botnets appeared to be technologies that, first, prevented bots getting onto end-user systems, and, second, detected bots running and alerted users to the problem.

The latest Mac operating system, Leopard, would raise the bar for security. Technologically it was on a par with Windows Vista, assuming Vista did everything it was supposed to do—but it was ahead on ease of use.

Cisco Systems

The Committee met Laura K Ipsen, VP of Global Policy and Government Affairs, and John Stewart, VP and Chief Security Officer. They argued that the industry was still inexperienced in understanding what the Internet meant for society. Practice varied: Microsoft had begun by focusing on usability, later on reliability, and now on security. In this respect the market had proved effective—the danger was that regulation would not be able to keep up as effectively with the developing threats. The market was very different to that for cars, where the technology, and the risks, were very stable and well-known.

There were only six or seven operating system vendors, and their security was improving. The challenge would be to reach the thousands of application vendors, whose products were increasingly targeted by the bad guys. The Government should focus on setting and applying penalties for those who abused the system; the role of industry should be to educate users. Time, and the development of the younger generation, would solve many of the problems. At the same time, standards of privacy would change.

Increasing volumes of data on the Internet were good for Cisco's business, but the volumes of bad traffic carried a cost in reducing the usability of many parts of the Internet. On internal Cisco security, Mr Stewart confirmed that routers did provide the facility of two-factor authentication, but that this was only advised as best practice, not mandated. Cisco's approach was to provide the capability, but not to dictate the implementation by ISPs.

More broadly, the motives and incentives to fix security problems were very involved. Most users did not know what a botnet was. If they got a message saying they were linked to a botnet they would just ring the helpline, so impacting on, for instance, Apple's profits. The best approach was not to focus on technological risks in piecemeal, when these were constantly changing, but to track down and prosecute the criminals.

Lunch

Cisco Systems hosted a lunch for the Committee and the CyberSecurity Industry Alliance (CSIA). Attendees were Pat Sueltz, Max Rayner, Matt Horsley and Amy Savage (all from SurfControl), Ken Xie (Fortinet), Kit Robinson (Vontu), Adam Rak (Symantec) and Thomas Varghese (Bharosa).

In discussion, attention was drawn to the number of reports of Internet crime on the IC3 website, and it was argued that this represented the tip of the iceberg. The only reliable thing about the data was the rate of increase—the actual figures were grossly under-reported. Overall, the position appeared to be getting worse rather than better. Although there had been no major outbreaks in the last year or two,

this was attributed to the fact that criminals increasingly chose to remain out of sight, using botnets to make money rather than distributing high-profile viruses.

Asked whether there was a down-side to security breach notification laws, it was suggested that some companies might not monitor breaches in order to avoid a duty to report them—the law should include a duty to monitor as well as to report. In addition, those receiving notifications should be given better information on what to do about them. More broadly, the effect of breach notification laws was seen as positive, but there was a view that they should be extended to cover printed as well as electronic material. Most security breaches remained physical, for instance employees losing laptops etc. Finally, it was argued that any such laws in the UK should not repeat the mistakes made in some US states, by making it clear that the duty to notify was universal, rather than being focused on UK citizens.

There was some discussion on overall responsibility for security. On the one hand it was argued that too much responsibility was being placed on end users—as if they were to be required to boil or purify water to avoid being poisoned, when in fact the infrastructure itself was the source of contamination. ISPs in particular should take a greater role in filtering traffic. On the other hand, it was argued that the analogy with water was misleading, as there was no consensus in the Internet field on what was "toxic".

eBay

Matt Carey, Chief Technology Officer, welcomed the Committee. Rob Chesnut, Senior Vice President, Trust and Safety, said that he had formerly been a federal prosecutor; several other former federal law enforcement officers worked for the company. He argued that eBay had a very strong incentive to improve security, as the company's whole business model was based on trust and the fact that customers had a good experience of the site.

Law enforcement was a key challenge: scammers might be deterred if they thought there was a chance of going to jail. The fact that Internet fraud crossed jurisdictions created difficulties, and authorities in some countries simply weren't interested in pursuing offenders. eBay devoted considerable resources to building up relationships with law enforcement around the world, providing advice, records and testimony as required. The company had played a part in over 100 convictions in Romania alone.

eBay also reported all frauds to the IC3 website, and encouraged customers to do the same—this meant that the IC3 data (showing 63 percent of complaints related to online auctions) were skewed. However, this reporting was essential to allow individually small individual cases to be aggregated. In addition, the company provided training to law enforcement, and hotlines that officers could call.

The number one problem facing eBay was phishing, which undermined confidence in the company and in e-commerce. eBay was targeted because it had the highest number of account holders, and therefore the best rate of return, and because holding an eBay account generated trust—which the scammers could make use of. eBay was working to make stolen accounts worthless, by detecting them and locking them down. However, the victims did not seem to learn from their mistakes—they would give up account details time after time. Most cases involved cash payments, e.g. via Western Union, rather than credit cards or PayPal.

The most worrying trend was the increased popularity of file-sharing. People did not appreciate the risk that the bad guys could then go on to search all the data in their personal files for account details, passwords and so on.

The company's major recommendations would be as follows:

- Provision of better training for law enforcement.
- Diversion of resources within law enforcement towards combating e-crime.
- Reappraisal of the penalties applied to those convicted of e-crime.
- Relaxation of the laws of evidence, to make the giving of affidavits or testimony by victims in different jurisdictions more straightforward.
- Aggregating of offences across jurisdictions.
- A requirement that money transfer companies prove the ID of those using their services.

Redmond, Friday 9 March

Microsoft

Security

Doug Cavit, Chief Security Strategist, drew attention to the powerful economic motivation to encourage Internet use. Security was key to this. At the same time, software development differed from, say, car manufacture, in that software was adaptive—it was not just a case of adding features at a fixed cost, but of an incremental process of development and manufacture.

Asked whether ISPs could do more, he noted that most ISPs currently isolated machines detected as belonging to botnets. However, actually contacting owners to fix the problem was too expensive. Microsoft offered a "malicious software removal tool" (MSRT) free of charge, which had been available for a year. Data on use were published.

The nature of the threat had changed. It was now about making money and, to some extent, attacking national security. Those behind the threat were expert and specialised. Attacks were moving both up and down the "stack"—exploiting on the one hand vulnerabilities in the application layer, and on the other working down through chips and drivers to hardware exploits. As a result traditional defences, anti-virus software and firewalls, were no longer adequate—every layer of the system now had to be defended. MSRT data also showed that there were now relatively few variants on viruses; on the other hand there were thousands of variants on back-door or key-logger exploits, designed to get around anti-malware programmes.

More broadly, the Microsoft platform had always been designed to enable interoperability and innovation. This would continue, though within Vista every effort had been made to ensure that the prompts and questions for end-users were more transparent.

Identity Management

Kim Cameron, Identity and Access Architect, said that he remained optimistic about the Internet. The more value was transferred through the medium the more

criminals would target it, but the industry could stay of top of the problems. The major companies were increasingly realising that they needed to work together and with governments—solutions to the problems were not purely technical. There had in many cases been a disconnect between the technology industry and governments. In the UK, for instance, the original, centralised proposals for ID cards had been very unfortunate, and the movement towards a more decentralised, compartmentalised system was very welcome.

It was possible to produce devices which were 100 percent secure. The problem came with the interaction between those devices and their human users. There were things that users should not have to know—the technical approach had to adapt to them. For instance, Windows had translated complex and, to most users, meaningless tasks into easily grasped visual analogies. The key challenge he faced was to translate identity management into similarly transparent visual terms. The image being used in CardSpace was of a wallet, containing multiple identities, from which, like credit cards, users could choose which one to use in particular circumstances.

The Internet had been built without an identity layer, and filling this hole retrospectively was a hugely complex task. The need to take on this task had to be accepted across the industry, and across national and political boundaries. Dr Cameron's paper on the Laws of Identity sought to achieve this by setting out key principles.

Emerging technologies such as RFID tags would have many potentially dangerous applications. It was essential that all such devices be set up in such a way that the individual had a choice over whether or not to broadcast his or her individual identity. The company was working on IP-free approaches to these issues, which would be available for other companies to develop in order to plug into their systems.

Privacy

Sue Glueck, Senior Attorney, and Nicholas Judge, Senior Security Program Manager, argued that security and privacy were two sides of the same coin. As well as improving security Microsoft had to invest in privacy, both to protect itself legally and to make deployments more straightforward.

Microsoft's public guidelines for developing privacy-aware software and services had been made public in an effort to help the computer industry, particularly smaller companies who could not afford to have full-time privacy and security staff, use a common set of rules and way of doings things. In this way some of the data breaches and other privacy problems that were currently widespread could be avoided. The guidelines were available for download at http://go.microsoft.com/fwlink/?LinkID=75045.

The company's key principle was that Microsoft customers be empowered to control the collection, use and distribution of their personal information. The company employed 250 staff to implement this principle, assessing each feature of software at an early stage of development against core privacy criteria. In the case of Vista, there were around 520 teams working on features, of which about 120 had privacy impacts. The requirement for privacy drove around 30 significant design changes. The privacy team was formerly seen as a nuisance, but increasingly designers and developers had bought into the value of privacy.

On the use of language, messages were tested against stringent usability criteria, including invented personae with varying knowledge of computers. However, the team did not have the resources to test messages against focus groups.

Questioned on the privacy implications of the Microsoft phishing filter, it was noted that the data sent to Microsoft were stripped of all log-in details and were only preserved for 10 days on a separate server.

Spam

Aaron Kornblum, Senior Attorney, said that Microsoft's Legal and Corporate Affairs Department had over 65 staff worldwide, seeking to use civil litigation to enforce Internet safety rules. The staff were in some cases recruited from government agencies, such as the FBI, the Metropolitan Police etc., but outside counsel were also used to bring cases.

Under federal and state laws ISPs could bring cases against spammers on behalf of their customers. Microsoft, through its ISP, MSN, had brought such cases.

In order to prevent phishing sites using the Microsoft identity, all newly registered domain names held by the registrars were scanned against key text, such as "msn.com". As a result of this work, along with a proactive approach to investigating, prosecuting and taking down phishing sites, the number of spoof MSN sites had fallen considerably. Prosecutions in such cases were launched under trademark law.

Partnerships with law enforcement were crucial, such as "Digital PhishNet", set up in 2004. Investigations were frequently worldwide, involving multiple lines of inquiry—for instance, investigating where phished data were sent, where phishing sites were hosted, and so on.

Looking forward, the key issues of concern were the prevalence of botnets to distribute malicious code, and the introduction of wireless technologies.

Linda Criddle, Look Both Ways

At a separate meeting, Linda Criddle drew attention to five factors that increased the risks to personal safety online:

- Lack of knowledge;
- Carelessness;
- Unintentional exposure of (or by) others;
- Technological flaws;
- Criminal acts.

Software was not currently contributing to safety, and in many cases was undermining it. Networking sites such as MySpace or espinthebottle did not default to safe options, encouraged the disclosure of personal information, the use of real names, and so on.

In addition, much content filtering technology only filtered external content. For example MSN content filtering did not filter the (often age-inappropriate) content of the MSN network itself. This left users wholly exposed.

Products should not carry a default risk setting. Wherever a choice was involved users should be fully apprised of the risks so that informed choices could be made.

APPENDIX 6: VISIT TO METROPOLITAN POLICE SERVICE, COBALT SQUARE

19 April 2007

Members of the Sub-Committee present were Lord Broers (Chairman), Lord Harris of Haringey, the Earl of Erroll, Baroness Hilton of Eggardon, Lord Mitchell, Lord O'Neill of Clackmannan, Dr Richard Clayton (Specialist Adviser), Christopher Johnson (Clerk) and Cathleen Schulte (Committee Specialist).

The Committee was welcomed by Detective Chief Inspector Charlie McMurdie, Head of the MPS Computer Crime Unit. The Committee then heard presentations from:

- Detective Sergeant Clive Blake (Computer Crime Unit);
- Detective Sergeant Stephen Truick, (the "Fraud Alert" site);
- Mark Wilson (Evidential Analysis);
- John Jack (Computer Systems Laboratory);
- Detective Inspector David Perryman (Professional Standards);
- Detective Sergeant Shaun Reardon (Counter Terrorism Command).

The Committee then toured the Computer Crime Unit and Child Abuse Command.

APPENDIX 7: GLOSSARY

419 fraud

Form of advance fee fraud, in which the victim is persuaded to put down a sum of money in anticipation of a much larger gain, which then fails to materialise. Named after the relevant article of the Nigerian criminal code.

Abstraction [of network layers]

Principle that there are different layers in a network and each one has a specific function, with clear boundaries between adjacent layers.

Botmaster

Controller of a botnet.

Botnet

Collection of compromised computers (individually called robots or zombies) running malicious programs that allow them to be controlled remotely; commonly used to distribute spam or launch Distributed Denial of Service attacks.

Browser

Computer program which permits the viewing of material on the World Wide Web.

Can-Spam Act

2003 Act of the United States Congress designed to regulate the use of spam.

Cybercrime

See e-crime.

Distributed Denial of Service attack

Attack launched by means of compromised systems (typically controlled via botnets), designed to overwhelm a particular servers or networks by flooding them with packets of information.

Domain

Name identifying a computer or computers belonging to a single organisation on the Internet.

E-crime

Crime committed against or with significant use of electronic networks.

End-to-end [principle]

Principle that the network core should only carry traffic, and that additional services should be delivered at the edges of the network, by end-points, not within the network core.

Exploit

Known way of taking advantage of a security problem with a system on the Internet.

File sharing

Practice of making files available for others to download over the Internet.

Firewall

Device controlling the passage of data between areas of a network that are more or less trustworthy.

Hacker

Person who tests out computer security, whether lawfully or unlawfully (e.g. for research, or for criminal purposes).

Hypertext

Text on a computer that leads the user to other information, e.g. by means of a "hyperlink".

Instant Messaging

Real-time communication between users of a network, by means of typed text.

Internet

The global network of interconnected networks that transmits data by means of the Internet Protocol.

Internet Protocol

Protocol for communicating data via the Internet using packet-switching.

Internet Relay Chat

Form of real-time Internet communication via dedicated channels.

Keylogger

Program that surreptitiously captures a user's keystrokes so that a remote attacker may learn passwords etc.

Level 1/2/3 crime

Crime that affect a local police force only (level 1); that crosses force boundaries (level 2); or that is committed nationally or internationally (level 3).

Malware

Malicious code.

Man in the middle

Attack in which the attacker places himself between two parties, e.g. the individual end-user and his bank, without those parties being aware that the link between them has been compromised.

Network

Interconnected group of computers.

Node

Device within a network.

Operating system

Program that manages the hardware and software resources of a computer.

Operation Ore

Police investigation into over 7,000 individuals in the United Kingdom whose details were found on a database held by Landslide Inc, an American company offering access to child abuse websites.

Packet

Block of data carried by a computer network.

Packet switching

Paradigm for communicating information by which communications between end-points are broken down into packets, and then routed between the nodes making up the network, before being reconstructed at the destination end-point.

Patch

Piece of software designed to fix a software vulnerability.

Peer-to-peer

Network in which participants share files or bandwidth, all participants being equals, rather than communicating through a central server.

Phishing

Criminal activity that relies on social engineering to persuade victims to enter user names, passwords etc on a spoof website.

Protocol

Set of guidelines governing communication between computers.

Root [name server]

One of the thirteen servers that answer requests for the "root domain" (the empty sequence at the end of every domain name) and redirect such requests to the "top level domain" (e.g. ".uk" or ".com") name-servers.

Router

Device that determines the proper path for data to travel between networks.

Sand-box

Virtual container in which programs that are not trusted can safely run within infecting the rest of the computer or network.

Spam

Unsolicited bulk email messages.

Spoofing

Launching an attack by masquerading as someone else.

Toolkit

A set of inter-related programs for a particular purpose, such as the production of malware or the incorporation of exploits into a Trojan.

Tor

The Onion Router, a system allowing users to communicate anonymously on the Internet.

Trojan [horse]

Program that installs malicious software, under the guise of doing something else.

Two factor [authentication]

Authentication requiring two different methods to be used, typically something known (a password) and something owned (often a key-fob generating a random sequence of six-digit numbers).

Vendor

Manufacturer of software or some other product.

Virus

Malicious program, attaching itself to an existing program, which can copy itself and infect or corrupt computers without the knowledge or permission of their owners.

Vulnerability

Weakness in a system that exposes it to attack.

WiFi

Wireless communications medium used by mobile computing devices.

World Wide Web

System of documents, identified or located by means of Uniform Resource Identifiers (that is, strings of characters used to specify particular resources or pages), interlinked by means of hypertext, and accessed via the Internet.

Worm

Malicious program that replicates itself and sends copies to other computers, so endangering the network by consuming bandwidth, but which does not need to attach itself to an existing program and may or may not corrupt the host computer itself.

Zombie

Compromised machine controlled by an external source, typically forming part of a botnet.

APPENDIX 8: LIST OF ACRONYMS AND ABBREVIATIONS

ACPO	Association of Chief Police Officers
APACS	Association for Payment Clearing Services
ARPANET	Advanced Research Projects Agency Network
ATM	Automated Teller Machine
CD	Compact Disc
CMA	Computer Misuse Act 1990
BGP	Border Gateway Protocol
BSI	British Standards Institute
CEOP	Child Exploitation and Online Protection Centre
CERN	Central European Research Network
CITRIS	Center for Information Technology Research in the Interest of Society
CSO	Chief Security Officer
DDoS	Distributed Denial of Service
DG	Directorate General
DoS	Denial of Service
DTI	Department ofTrade and Industry
EFF	Electronic Frontier Foundation
EURIM	European Information Society Group
FBI	Federal Bureau of Investigation
FIPR	Foundation for Information Policy and Research
FSA	Financial Services Authority
FTC	Federal Trade Commission
IC3	Internet Crime Complaint Center
ICO	Information Commissioner's Office
ICT	Information and Communication Technologies
IP	Internet Protocol
IRC	Internet Relay Chat
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IT	Information Technology
ITSPA	Internet Telephony Service Providers' Association
IWF	Internet Watch Foundation
JANET	Joint Academic NETwork
LINX	London Internet Exchange

LTSS	Local Trading Standards Services
MPS	Metropolitan Police Service
MSN	Microsoft Network
MSRT	Malicious Software Removal Tool
NEN	National Education Network
NHTCU	National High Tech Crime Unit
OFT	Office of Fair Trading
PATS	Publicly Available Telephone Service
PC	Personal Computer
PGP	Pretty Good Privacy
QCA	Qualifications and Curriculum Authority
RCFL	Regional Computer Forensic Laboratory
RCUK	Research Councils UK
RFID	Radio Frequency Identification
SCL	Society for Computers and Law
SMS	Short Message Service
SOCA	Serious Organised Crime Agency
Tb	Terabyte (10^{12} bytes)
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VoIP	Voice over Internet Protocol