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.

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.

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.

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.

2.37. 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.

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).

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

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

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.**

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

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

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.

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.**

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

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.

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.

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.

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

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.**

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