HOUSE OF LORDS

Science and Technology Committee

4th Report of Session 2007–08

Personal Internet Security: Follow-up

Ordered to be printed 24 June 2008 and published 8 July 2008

Published by the Authority of the House of Lords

London : The Stationery Office Limited
£price

HL Paper 131

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 (co-opted)
Lord Colwyn
Lord Crickhowell
Earl of Erroll (co-opted)
Lord Haskel
Lord Howie of Troon
Lord Krebs
Lord May of Oxford
Lord Methuen
Earl of Northesk
Lord O'Neill of Clackmannan
Lord Patel
Earl of Selborne
Lord Sutherland of Houndwood (Chairman)
Lord Taverne
Lord Warner

For membership and declared interests of the Sub-Committee which conducted the original inquiry, see the Committee's 5th Report, Session 2006–07, *Personal Internet Security* (HL Paper 165).

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 to 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: Reference 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

Personal Internet Security: Follow-up

THE COMMITTEE'S COMMENTARY ON THE GOVERNMENT RESPONSE

Background

1. In August 2007 we published our Report *Personal Internet Security*.[1] We made a number of recommendations, the underlying principle of which was that although the Internet was a powerful force for good, action had to be taken quickly to ensure that, in a period of rapid technological change, members of the public had confidence that the Internet was safe and secure and that personal data were properly protected.

2. The Government responded in October 2007 (Cm 7234). They did not share our view that there was a public perception of the Internet as a lawless "wild west" and many of our recommendations were rejected.

3. Given this unsatisfactory response, on 20 February 2008, we announced a short follow-up inquiry. We wrote to those who had given oral evidence to our original inquiry and asked them to comment on the Government response. We are grateful to those who replied and their replies are printed as evidence at the end of this Report. Following the written consultation, on 20 May, we took oral evidence from two Ministers involved in Government policy on personal Internet security: Mr Vernon Coaker MP, Parliamentary Under-Secretary of State for Crime Reduction at the Home Office, and Baroness Vadera, Parliamentary Under-Secretary of State for Business and Competitiveness at the Department for Business, Enterprise and Regulatory Reform. A transcript of their evidence is reprinted in this volume.

Our follow-up inquiry

4. Follow-up inquiries, whether undertaken soon after publication of the original report or after a more substantial period of time has lapsed, are an important part of the scrutiny activity of the Science and Technology Committee. On this occasion, we were pleased that, following the disappointment of the Government's original response, Ministers were able to offer a slightly more positive view of how the Committee's recommendations were to be taken forward. We were heartened by Mr Coaker's acknowledgement that our follow-up inquiry had prompted the Government to re-consider their response—not only had the Committee's report "helped to drive the agenda forward" but "the re-submission of evidence and the re-thinking that that [had] caused" had reinforced that progress (Q 24).

5. Whilst we welcome this comment, the evidence we received during this short follow-up inquiry indicates that there is still much work to be done, and that the Government's assertion that they are driving forward the personal

[1] House of Lords Science and Technology Committee, 5th Report, Session 2006–07 (HL Paper 165).

Internet security agenda is more a matter of promises for the future than achievements in the present.

6. We draw in particular the following areas of concern to the attention of the House.

Responsibility for personal Internet security

7. In our Report we concluded that that the emphasis of Government and policy-makers upon end-user responsibility for security bore little relation either to the capabilities of many individuals or to the changing nature of the technology and the risk. We recommended that the Government should develop a more holistic understanding of the distributed responsibility for personal Internet security (Recommendation 8.7).

8. We welcome Baroness Vadera's clarification that it was not her department's view that consumers had "ultimate responsibility" (Q 2) and also her acknowledgment that the Government needed to show "some leadership" in this area (Q 3). It remains disappointing however that despite the Government's commitment to work with the industry to promote consumer confidence in the role of Internet Service Providers (ISPs) in ensuring personal Internet security, we heard no evidence from the Government of any concrete developments. **We take some comfort from Baroness Vadera's agreement that measures need to be introduced to protect the consumer against e-crime, demonstrated by her expression of interest in kite-marking and a code of conduct for ISPs. We look forward to positive achievements in this regard in the near future.**

Software vendor liability

9. In response to our recommendation (Recommendation 8.15) that the general principle of software vendor liability should be explored, the Government suggested that there was scope for this matter to be raised during discussions at the European level on the Review of the Consumer Acquis. We asked Baroness Vadera for a progress report. We were disappointed to be told that software vendor liability was unlikely to be taken up in those discussions (Q 7). This answer however came as no surprise since we had received evidence from Nicholas Bohm, one of the expert stakeholders accredited to the European Commission in connection with the Consumer Acquis review, that he had not been aware of any discussion about changing the liability model applying to vendors, either at the European level or in meetings between United Kingdom stakeholders and the Ministry of Justice (p 22).

10. We acknowledge that steps to establish software vendor liability should be taken internationally, rather than by the United Kingdom alone. **We therefore press the Government to indicate how they intend taking this recommendation forward if their original intention with regard to the Consumer Acquis discussions have proved unfruitful**.

Protection of personal data

11. The protection of personal data was national news in November 2007 when it became public that there had been a serious security breach at Her Majesty's Revenues and Customs (HMRC). Two computer disks containing HMRC's child benefit database were sent to the National Audit Office but went missing in transit. Personal data, including bank account details,

affecting about 25 million people were lost. In a recent report by the Joint Committee on Human Rights (JCHR), further lapses in personal data security by the Government are enumerated. They include, for example, "the theft of a Ministry of Defence laptop containing personal information relating to around 600,000 people, most of whom had expressed an interest in joining the Royal Navy, Royal Marines or the Royal Air Force" and "the loss of two disks in transit from the Driver and Vehicle Agency in Northern Ireland to the Driver and Vehicle Licensing Agency in Swansea, containing the unencrypted details of 7,500 vehicles and the names and addresses of their owners".[2] The JCHR concluded that "it would be wrong to see these errors and lapses as unfortunate 'one-off' events. In our view they are symptomatic of the Government's persistent failure to take data protection safeguards sufficiently seriously … The rapid increase in the amount of data sharing has not been accompanied by a sufficiently strong commitment to the need for safeguards."[3]

12. Baroness Vadera's view that the HMRC incident was "a bit of a wake-up call" (Q 13) seems to us to be an understatement of the seriousness of what has been happening within Government. In his follow-up submission, Nicholas Bohm comments that "the Committee's concerns have turned out to be well-founded; and the Government's denials that losses of personal data were increasing or that it was indifferent to them have been cast into the awkward light of reality by the deluge of reported data losses that began to emerge in such quantity not long after its reply was published" (p 22). More positively, the Metropolitan Police Service suggests that "the benefit of these recent catastrophic losses may be to force industry to examine their own protection systems and processes" (p 29).

13. We regret that what in fact appears to have been a level of indifference on the part of the Government has now been dispelled only as a result of recent incidents involving serious losses of personal data. As Mr Richard Thomas, Information Commissioner, told the JCHR: "it should not take a train crash to prevent casualties on the railway, but we have had a train crash and that has served as a wake-up call".[4]

14. The Government set up a number of reviews to improve their performance with regard to personal data security: the Cabinet Secretary, Sir Gus O'Donnell, established a review into data protection and security procedures within government;[5] Kieran Poynter, Chairman and Senior Partner of PricewaterhouseCoopers LLP, carried out a review of data handling in the HMRC;[6] Sir Edmund Burton, Chairman of the Information Assurance Advisory Council, carried out a review within the Ministry of Defence,[7] and the Information Commissioner and Dr Walport, Director of the Wellcome

---

2 Joint Committee on Human Rights, 14th Report, Session 2007–08, *Data Protection and Human Rights* (HL Paper 72) (HC 132), p 5.

3 *Ibid*, p 14.

4 *Ibid*, Q 137.

5 *Data Handling Procedures in Government: Final Report*, Sir Gus O'Donnell (published 25 June 2008). See http://www.cabinetoffice.gov.uk/

6 *Review of information security at HM Customs and Revenue*, Kieran Poynter (published 25 June 2008). See http://www.hm-treasury.gov.uk/independent_reviews/poynter_review/poynter_review_index.cfm

7 *Report into the Loss of MOD Personal Data*, Sir Edmund Burton (published 25 June 2008). See http://www.mod.uk/DefenceInternet/AboutDefence/CorporatePublications/PolicyStrategyandPlanning/ReportIntoTheLossOfModPersonalData.htm

Trust, are looking at the framework for the use of information in both the private and public sectors. In a letter dated 3 June, Baroness Vadera provided further information about the reviews: "the Government", she says, "will take a considered view on what further measures it needs to take to strengthen the protection of personal data in light of the recommendations" of the four reviews. The letter is printed with this Report (p 14).

15. As for action by the private sector, we note that in their follow-up submission, the Association for Payment Clearing Services (APACS) indicates that their members and the wider banking community are also involved in initiatives to strengthen the arrangements for the protection of personal data. Baroness Vadera, however, speaking more generally about businesses, was less upbeat: although there was a trend of increasing spend on IT security, about 20 per cent of companies, she said, spent less than one per cent of their IT spend on security. She concluded that there was more to be done (Q 13), and we share that view.

16. **We look forward to an early report to the House about the measures that will be put in place by the Government, in light of the outcome of the various reviews that have been undertaken, to strengthen personal data security both within Government departments and also within the business sector.**

17. In our Report we also recommended that the Government accept in principle that a data security breach notification law was needed, and that they should begin consultation on its scope (Recommendation 8.18). We characterised this as being "among the most important advances that the United Kingdom could make in promoting personal Internet security". The majority of the follow-up submissions comment upon our recommendation, with many concerns being expressed about the potential scope, but equally noting that we had already been careful in Recommendation 8.19 to address some of the potential pitfalls. Baroness Vadera's view was that it was very difficult to draft legislation or regulations that would set the correct level at which individuals should be informed about a breach—it was "really about proportionality and significance" (Q 16). She also told us that this issue would be considered as part of the reviews of Government data security.

18. **We entirely agree that setting the correct level of notification is absolutely key, but we hold to our view that data security breach notification legislation would have the twin impacts of increasing incentives on businesses to avoid data loss, and should a breach occur, giving individuals timely information so that they can reduce the risk to themselves.**

Consumer protection

19. We recommended (Recommendation 8.17) that legislation should be introduced to establish the principle that banks be held liable for losses incurred as a result of electronic fraud. The Government responded that this would be an inappropriate approach to securing liability and that the Banking Code offered sufficient protection against losses arising from fraud, a point also taken up by APACS (p 18).

20. We find this response wholly unsatisfactory. Professor Ross Anderson (p 15) and Nicholas Bohm (pp 22–23) in their follow-up submissions are critical of the Government's reliance on the banking industry. Professor Anderson says:

"on consumer protection, the Government is being disingenuous in claiming that the banking industry's practices provide adequate protection". He goes on to argue that "the banking code … provides scant protection; where a password or PIN has been used, the bank often simply claims that the customer must have been negligent or complicit" although there were a variety of means by which passwords and PINs could be harvested without the customer being aware. The Financial Services Ombudsman (who "routinely backs the banks") and the courts, he suggests, do not provide adequate avenues for redress and, as a result, "dozens of victims" approach him every year "out of desperation" (p 15).

21. Nicholas Bohm makes a similar complaint that "the banks' 'proof' that the customer colluded in the fraud or caused it by negligence is a proof by assertion not based on evidence openly produced for testing" (p 22). He goes on to point out that the banks design the systems for online banking, and "if they were forced to meet claims that they could not disprove by open evidence, they could decide whether to stand the losses or to improve the security, whichever they preferred". (p 23)

22. **We remain strongly of the view that the liability of banks for losses incurred by electronic fraud should be underpinned by legislation rather than by the Banking Code, and we urge the Government to review their response to our recommendation without delay.**

23. **We also have significant concerns about the way in which complaints of online banking fraud are currently handled and, in particular, the basis on which the banks determine that an alleged fraud is to be attributed to the customer, whether by fraudulent or negligent activity. We recommend that the banks' approach to handling allegations of online fraud should be reviewed as a matter of urgency.**

Reporting procedure for online fraud

24. In our Report we expressed surprise at the decision of the Government to issue guidelines (with effect from 1 April 2007) to police forces as a result of which those who had experienced online fraud were encouraged to make a report in the first instance to APACS who would then decide whether to forward the report to the police. We were concerned about reporting fraud in this sequence on the ground that the decision of the banks to pass a report to the police might be influenced by commercial factors. We recommended that the Government should review these guidelines as a matter of urgency (Recommendation 8.27).

25. Nicholas Bohm expresses a similar concern: "The Government claims that where customers are not refunded they retain the ability to report these matters directly to the police, where crimes should be recorded. I am sceptical of this latter claim, and suspect that where the bank refuses to report a fraud, the police may well refuse to accept the customer's claim that there was one … A system which depends on a decision by a bank on whether or not a customer has been defrauded is flawed by the fact that the bank has a direct financial interest in denying the customer's claim" (p 23).

26. In their original response, the Government did not accept our recommendation on the reporting procedure, arguing that the current arrangement significantly reduced police bureaucracy without compromising their effectiveness in dealing with online fraud. **We are pleased therefore**

that the Government have reflected further on this matter and have now undertaken to review the reporting procedure to "see whether it [is] working in the way that [the Government] intended" (Q 43). Meanwhile, we reiterate our strongly held view that the current reporting sequence is wholly unsatisfactory and that it risks undermining public trust in the police and the Internet.

Data collection and a classification scheme for recording of e-crime

27. In our Report we recommended that there should be a more co-ordinated approach to data collection relating to e-crime, including the development of a classification scheme for recording all forms of e-crime (Recommendation 8.3). We proposed that the classification scheme should cover both Internet-specific crimes (such as Distributed Denial of Service attacks) and also e-enabled crimes (traditional crimes committed by electronic means or where there is a significant electronic aspect to their commission). The Government did not accept our recommendation, arguing that e-crimes are "standard offences that are facilitated by new technology, rather than new types of offence".

28. We share with Nicholas Bohm, a member of the Law Society's Electronic Law Committee but commenting in his personal capacity, the view that the Government's response "misses the point" because "what e-crimes have in common is that they require particular skills to investigate them" (p 20). A number of others also feel that the Government should have responded more positively to our recommendation. APACS comment in the same vein as Nicholas Bohm and encourage us to "create the conditions for policy makers to better understand the impact of e-crime" (p 16). eBay and PayPal suggest that collection and classification of e-crime data would "provide a helpful tool for companies actively fighting e-crime … and would also be helpful in shedding light on the real scale of the problem" (p 26). The Children's Charities' Coalition on Internet Safety (p 26) and the Child Exploitation and Online Protection Centre (p 25) make a similar point.

29. Given this level of disagreement with the Government response, we were pleased to hear a more encouraging response from Mr Coaker who explained that there were proposals under consideration to develop the National Fraud Reporting Centre (NFRC), announced in March 2007 following the 2006 Fraud Review, as a focus for collecting information about all frauds, both e-crime and traditional, and also about those crimes which were not fraud but were e-crime (Q 24).

30. **The availability of comprehensive and reliable data about e-crime—the scale of the problem, the risks to the public and the costs to the economy—is fundamental to developing an effective response to the problem of e-crime and to promoting public confidence in the Internet. We urge the Government to implement proposals in response to our recommendation on data collection and data classification without further delay.**

Police Central e-Crime Unit

31. In our Report we urged the Home Office to provide funding to accelerate the establishment of the Police Central e-Crime Unit since at the time when the Report was agreed (in July 2007) there had still been no funding

commitment (Recommendation 8.29). This recommendation is firmly endorsed by Symantec in their follow-up submission (p 32).

32. The Government responded positively to our view that there should be national co-ordination of policing e-crime, recognising that "such crime is not a problem that sits comfortably within local policing structures, and … historically most forces have underinvested in their capacity to respond effectively to it"; and in evidence, Mr Coaker reiterated the Government's belief that there was a "gap"—"a gap without a shadow of a doubt" (Q 33)—in the coordination of law enforcement in this area. As for funding, Mr Coaker told us that "within reason" the Home Office would "look to fund [a] law enforcement capability alongside the National Fraud Reporting Centre" (Q 33). He said that he would be meeting relevant law enforcement agencies to discuss this matter on 4 June. We understand that the law enforcement agencies present (Association of Chief Police Officers/Metropolitan Police Service, Serious Organised Crime Agency and City of London Police) reported to Mr Coaker that they had made good progress in working together to develop the law enforcement response to e-crime reported through the NFRC. The group will meet again in July to update Mr Coaker on progress.

33. **Whilst the Government appears to be moving in the right direction with regard to co-ordinating the policing of e-crime, we are concerned at the pace at which their commitment to develop a coordinated e-crime law enforcement capacity is proceeding. We invite the Government to report on the outcome of their meetings with relevant law enforcement agencies and to indicate by which date they anticipate a national e-crime law enforcement unit will be operative.**

International co-operation

34. In our Report we acknowledged that the United Kingdom was seen as a "good partner" in international action on e-crime but noted that the Government had yet to ratify the Council of Europe Convention on CyberCrime which the Government had signed in November 2001 (Recommendation 8.31). We believed this to be a matter of concern, particularly with regard to the mutual assistance provision set out in Article 25. **In evidence, Mr Coaker told us that there had been some delay but that they intended ratifying the convention by the end of 2008. We welcome this commitment.**

35. We also recommended that the Government review the procedures for offering mutual legal assistance (MLA) in international e-crime cases (Recommendation 8.31). The Government's response was that there was sufficient provision made within the Crime (International Co-operation) Act 2003. However, our concern had been the slowness of MLA procedures, and this was something picked up by a number of the follow-up submissions. APACS comments "we do not feel that current arrangements for mutual legal assistance are sufficient to deal with the phenomenon of e-crime" (p 20). The Metropolitan Police Service characterises the MLA process as being "too slow to secure 'real-time' and 'short-lived' evidence", and calls for a "comprehensive review of the process" (p 30). Mr Justin Millar, Head of Computer Crime at the Home Office, told us that relevant work was going on in the G8 hi-tech crime subgroup and the Council of Europe Convention

group (Q 49). **We are pleased to hear that the emphasis has moved on from putting mechanisms in place, to considering whether those mechanisms are operating in a timely manner.**

Conclusion

36. **We acknowledge that, following the Government's disappointing response to our Report, they have reflected further and, with regard to some of the issues we raised, there has been some progress towards meeting our concerns. What progress there is, however, appears to be slow. Given this, we particularly welcome Mr Coaker's offer to keep the Committee informed, every two months, of what is happening (Q 50). We accept this offer and look forward to the Minister's first report in July. We anticipate that we shall be returning to this topic on a regular basis.**

APPENDIX: LIST OF WITNESSES

The following witnesses gave evidence. Those marked with a * gave oral evidence:

Professor Ross Anderson

Association for Payment Clearing Services

Nicholas Bohm

The Child Exploitation and Online Protection Centre

The Children's Charities' Coalition on Internet Safety

* Mr Vernon Coaker MP, Parliamentary Under-Secretary of State for Crime Reduction

eBay and PayPal

The Metropolitan Police Service

* Mr Justin Millar, Head of Computer Crime (Home Office)

* Mr Geoff Smith, Deputy Director, Communication Supply, Department for Business, Enterprise and Regulatory Reform

Symantec

* Baroness Vadera, Parliamentary Under-Secretary for Business and Competitiveness

Minutes of Evidence

TAKEN BEFORE THE SELECT COMMITTEE ON SCIENCE AND TECHNOLOGY

TUESDAY 20 MAY 2008

Present	Crickhowell, L	Northesk, E
	Erroll, E	Sutherland of Houndwood, L (Chairman)
	Haskel, L	Warner, L
	Krebs, L	
		Harris of Haringey, L

Examination of Witnesses

Witnesses: MR VERNON COAKER, a Member of the House of Commons, Parliamentary Under-Secretary of State for Crime Reduction, MR JUSTIN MILLAR, Head of Computer Crime, Home Office and BARONESS VADERA, a Member of the House, Parliamentary Under-Secretary of State for Business and Competitiveness, MR GEOFF SMITH, Deputy Director, Communication Supply, Department for Business, Enterprise and Regulatory Reform, examined.

Q1 ***Chairman:*** May I welcome you and thank you very much for giving us your time to come to pursue this clearly very interesting and, from the front page of some of the papers, highly relevant topic this morning. It seems we never escape it; it is with us. I welcome too, members of the public who have come wanting to follow the proceedings as they have done very carefully in the past. May I remind you that it is of course all on the record? We have little signs out saying who we are, we know who you are and we do appreciate having two ministers at one meeting; it has taken some organising and your cooperation in this has been very helpful. What we would propose to do, unless either of you wanted to make any opening comment, is just move straight to the questions. Do either of you wish to make an opening statement?
Mr Coaker: No, thank you.

Q2 ***Chairman:*** May I take the first question and then we will simply move around the table with various items we want to raise? The original report that we put out was received with a lot of interest and indeed the specialist press especially took great care over some of the details in the report and the many recommendations that we made. I have to say some of us thought that the Government's response was just a little bit bland, which is one way of putting it, but we followed through, in the light not least of what has happened since then, some of the implications that have arisen for the issues that we were considering. We thought it timely to move now to further discussion and we would hope to put out a short follow-up report on this topic. Perhaps I can raise an opening question which is central to all the ground that we covered which is; in the end, who is finally responsible for personal Internet security? Is there a locus within the system, within Parliament or elsewhere, and, if not, is there someone who ought to be? We have seen various possibilities suggested; it is a matter for the individual, it is a matter for the ISP and so on, and we had our own recommendations on this. However, may I just open the discussion by asking who is responsible for personal Internet security?
Baroness Vadera: First of all, thank you very much for the report, because I found it very interesting and read it quite recently for the first time knowing that I was going to be here. The report, which was somewhat more interesting than our response, actually had it correctly pitched, that it is distributed responsibility and that some of it is quite structural to the sector, and there is quite a lot of complexity around this which the report actually discusses very well. I found the analogy of the road system quite compelling, even though, as you say, there is no perfect analogy. I saw in some of the discussions, that there was this view that you believed that we took the view that it was the consumer who was ultimately responsible. I certainly do not think that is true. I do not believe from the discussions that I have had within the department since that, that is the department's view, so I apologise if that was the view which came across. It is distributed; it does make it complex. There is the issue around both hardware and software vendors, and the security vulnerabilities appear to come much more around the software vendors and I know that there is an issue around what their liability is. There is an interesting view around ISPs and what they have to do and there is possibly more that we could do around that. There is the Government and the consumer and of course the businesses ultimately and to try to impose, on what is quite a complex system, a single line of responsibility would have quite a lot of disadvantages which you actually explore in the report around inflexibility, inter-operability problems. Supposing you made the

software vendor liable, then you could end up with a system a little bit like we have on mobile phones, which is that what is downloaded is what you get access to because, in one sense they do not control everything and they would need to control things if they felt they were liable. We do have the system that we have and we have to work to ensure that we raise the bar for each of those players.

Q3 ***Chairman:*** I would like to come to ISPs in just a moment, but one of the concerns we had was that the way the weight of the responsibility seemed to be distributed, was that there was a very large responsibility on the individual. This is a very complex world, that is one of the things we all discover the more we immerse ourselves in it. You did query whether or not we had got it right and we wondered whether the weight should really be significantly elsewhere. Yes, individuals have responsibilities; as with credit cards, they should not leave them lying around and leave their pin numbers written down and all that sort of thing. There are comparable issues here but it is a more complicated world.
Baroness Vadera: It is right that it cannot be weighted entirely towards consumers. As you say, it is not that they are necessarily the best informed. There is a difference, for example, when it comes to certain types of breaches of security. At the time you were doing the report, phishing was quite a big subject, but when there are things that are actually more around the behaviour of the consumer, you can see that actually they need to be careful. It is about actually listening to the fact that your bank has told you not to respond to that email, so that changes the level of responsibility. I would not say that this needs to be entirely weighted towards the consumer at all.
Mr Coaker: Yes, that is right.
Baroness Vadera: Certainly the Government needs to show leadership and there are some things that you suggest in the report that we need to look at. For example, you discuss a kite mark for ISPs which is interesting. I have been told since, that the BSI owns the kite mark as a concept but we might be able to look at things like a code of conduct that ISPs need to consider. We might be able to raise the game for software vendors by giving them, at the EU level perhaps, a sense of expectation of what the market will want from them so that they are not rushing things to market. Again on ISPs, we know that the ten major ISPs cover the majority, but there is a whole tail of other ISPs that we do not know about, which I know Vernon will have to worry about when it comes to things like what we have done recently. We maybe need to do some research and we need to show some leadership on this ourselves. The ISPs do do a fair bit and I have looked at some of the research which my officials showed me that showed that they do actually turn off contaminated users. I do not know whether that is the right terminology, but you know what I mean. There are things that people are in fact already doing. We know that increasingly hardware is actually sold with the software already bundled in, so there is a change and I would not want it to be believed that it was entirely an issue for the consumer but there are certain things that the consumer really needs to be aware of because there are certain things you cannot deal with in the software; they are about the way they actually use the system.

Q4 ***Chairman:*** On the question of kite marks, the Government's response suggested you were waiting for the EU regulatory framework and we understand that there is now a draft of that out. Has that moved things ahead? Has the consideration of that within Government taken place?
Baroness Vadera: There are two bits; I do not know which bit of the EU framework you are talking about. There are two separate things. There was the review of the Consumer Acquis where, it is fair to say, we are struggling to get the consumer side of this looked at but that is a separate issue. There is currently a framework discussion around telecoms; I was in fact in France yesterday having a discussion with the French minister responsible. They are going to take over the presidency of the EU starting on 1 July, but I am not sure that we will be covering ISPs in the regulatory framework in quite that way.
Mr Smith: May I just add something on the framework? One of the headline issues when the draft proposals were issued was that the Commission intended to increase the security of networks. The way those discussions have gone is focusing responsibility on network providers and service providers to protect personal information, interconnection points and maintain availability of networks. So the regulatory climate is changing and there will be increased expectations on ISPs and others from 2010 onwards. Negotiations are, of course, underway and we are nowhere near finished but the background is shifting to a more security-aware environment.

Q5 ***Chairman:*** Thank you, that was very helpful, but could you identify yourself for the record?
Mr Smith: I am Geoff Smith, I am Deputy Director, Communication Supply, in the Department for Business.

Q6 ***Lord Crickhowell:*** I was not on the Committee when this report was prepared, so I have picked it up, and I suppose I have picked it up as a consumer. As we started on consumers, I thought I would pick it up now, but I was pretty shaken by the statement right at the start of your response that the Government do

not agree with the implication that the public has lost confidence because of the increase in trading. Well, I am a pretty experienced computer user, I was chairman of an IT net company but certainly members of my family are worried and not a day goes by without several invitations, usually from banks, but from other organisations, for me to come back to them; very often banks with which I do not do business, so I never open them. Then I order something, probably asked to by my wife—I bought something on the Internet, as it happens, 48 hours ago from a European company—and up comes a security crosscheck. I may be familiar with the organisation that is doing it, but the ordinary consumer is expected, according to the Government, to realise that half these messages from apparently respectable organisations like major banks and building societies inviting them to provide security information or their account will be closed down, to know who the organisations are that are secure when they are asked to provide the financial information to complete their purchase. I do not believe that is fair on a huge number of new consumers. Surely there is a need to safeguard the consumer by providing much more information about who the kite-mark-approved people are and indeed we ought somehow to be able to stop all these extraordinary numbers of invitations which appear on our computers daily requesting information. If they are not from well-known banks, why is something not being done to get them off the system?

Baroness Vadera: Quite a lot of the ISPs have for starters very good systems on spam. I have a private account with an ISP, but I actually tend to find more of my emails are quarantined than spam; I end up in a situation where, actually, legitimate emails have been quarantined. So it is true and fair that people need to go with good ISPs who actually can filter emails and spam but at the end of it, if there is one basic instruction which is "Don't give out your password by invitation in an email", it is the same thing as "Don't leave your credit card lying around". There is some level of responsibility with consumers on that and I would suggest that. It is true though that the majority of transactions from banks are actually their responsibility, the reimbursement comes from the banks and they have actually therefore taken it more seriously and the level of bank security breaches has actually decreased recently. I am not going to vouch for the numbers because they come from the Banking Association so they are not our figures but it has gone down, they claim, to under £25 million when it used to be just over £30 million; it is reducing. We need to have a number of measures, including possibly the kite-marking or code of conduct with the ISPs, including making sure that banks feel a sense of responsibility, which they appear to, and the fact that consumers need to know a very basic thing. I understand it is problematic for them to recognise who is respectable and who is not respectable, for them to know not to voluntarily give somebody their password on an email is a legitimate thing to ask them to consider, and possibly for us to ensure that they are educated about.

Chairman: I have to say I cannot resist mischievously telling you that occasionally there is an over-zealousness in excluding emails and I have had the House of Lords computer exclude an email to me from the then Scottish Executive. Perhaps that was a political statement, I do not know.

Q7 ***Lord Haskel:*** Continuing with the interests of the consumer, in our report we recommended that there should be an exploration of the general principle of software vendor liability and, in the short term, that there should be liability for negligence. You responded that this was being discussed with the ongoing EU review of the Consumer Acquis. What is the position on this? Is it still on the "to do" list'? Is this something on the agenda for this meeting you were telling us about on 1 July?

Baroness Vadera: As I implied earlier, it is fair to say that, in terms of the EU review of the Consumer Acquis, we are not very hopeful that this will be taken up. However, we do understand and accept the whole issue of software vendor liability. It would be fair to say that there is more that we can do, but I would be reluctant to start with the proposition that we need to legislate and basically make them liable for a number of reasons. First of all, it is actually quite hard to have attribution of liability in a system—I actually learnt this from your report in the first instance and then explored it—because of the way the Internet works on layers—and actually to find a way in which you can be clear about the liability is very difficult. If we were, it would require a degree of control that the software vendor would need, which, in the report again, you slightly shied away from. You thought that was problematic, it would lead, like mobile phones, where you only have a certain type of software that is downloaded on it, to massive inter-operability issues. It would also be very difficult to do this on a UK level. This is a global industry. We do not have, in any shape or form, the majority of the vendor industry in the United Kingdom, so we need to be global and therefore one of the things that we were interested in doing was taking it up at the EU level. On the issue of negligence, the issue is whether you could prove negligence given the complexity of the system, but if you could, then there are common law protections. What we do need to do is to find a way, either a voluntary way or at the EU level, to raise the bar of expectation on the software industry, in particular this rush to market which has decreased, famously since the memo from Bill Gates, but decreased over time, that we ensure that there is an

expectation. There are also very interesting things that consumers are doing. I know that there is an issue around consumers that we discussed, but, for example, on the Microsoft Internet Explorer, that actually automatically downloads security updates every 30 days and there is an interesting thing going on, although I do not have the numbers, with a switch to an alternative, Firefox, because they do it every six days and people are beginning to become aware of that. So in one sense a bit of competition would be a good thing to make consumers feel more empowered. To start with the view that we need in the UK to have a regulation that is simply for the UK, I am pretty sure is not workable, but I know that we need to up the game and find alternatives.

Q8 ***Lord Haskel:*** In your response you said that there should be a debate to consider both how to improve the reliability of software and to protect the interests of consumers, while not reducing the quality of software available on the market or the incentives to innovate. It does seem to me that these are rather complicated and rather ambitious objectives. What actually are you doing to promote this, because this is part of all this business of protecting the consumer?
Baroness Vadera: We need to raise it at the EU level. I was in France yesterday and we did discuss this with the minister there; they have the French presidency. We need to do some very basic things around licensing agreements, for example. The National Consumer Council has referred 17 companies to the OFT for consumer licence breaches of some sort. Apparently, in some of these cases, you cannot actually read your licence agreement until after you have bought the product, which strikes me as slightly interesting and bizarre. So there are things that we can do but we do need to have a discussion and it does need to be at the EU level. Most of the software that is used is not produced in the UK, so we do need to have a discussion at a different level.

Q9 ***Lord Haskel:*** Is there going to be anything in the Bill that we were promised in the statement last week?
Mr Coaker: It is up for discussion but I do not know.
Baroness Vadera: It sounds like it is not because none of us is aware of it.

Q10 ***Chairman:*** "I do not know" is a good answer sometimes.
Mr Coaker: It is an early draft, if it is a draft at all.

Q11 ***Earl of Northesk:*** You mentioned automatic software updates. You will also be aware no doubt that over the past week or fortnight, Windows issued their SP3, Service Pack 3, update. That had the effect of freezing people out of their own computers and crashing those computers. It is all very well to say automatic updates are useful but they are not, because they have their problems. So the question I am really trying to drive at is that vendor responsibility and liability have to sit in there somewhere.
Baroness Vadera: I am sure the fact that they have crashed systems means they will be clearly liable, but one of the things that we do need to look at is the whole issue of what is expected of them as an industry and although the culture has changed quite significantly, there is still a slight sense of rushing the next thing to the market. I can only repeat what I said, which is that we need to have a clearer sense or expectation that this is not acceptable.

Q12 ***Earl of Erroll:*** I would like to mention that actually they do exclude liability, and what is worse is that the solution is to go online to get a fix and the trouble is they have just crashed, you so you cannot get back online so you are in a fix. Unless you know how to do rollback, there is not a lot you can do about it or it will be very expensive and it is a serious problem.
Baroness Vadera: Yes, I understand.

Q13 ***Lord Harris of Haringey:*** In our report, we said we wanted the Government to ensure " . . . the right incentives are in place to persuade businesses to take the necessary steps, to act proportionately to protect personal data". The Government's response said ". . . we do not accept that the incidence of loss of personal data by companies is on an upward path". Now clearly that response did not refer to government departments. However, I suspect that things that have happened since might mean that the response would be in different terms. We also recommended 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. You responded to that that the enforcement regime was fit for purpose. Given all that has happened, have the Government changed their position on any of this?
Baroness Vadera: It is fair to say that some of the data loss experienced by the Government has been a bit of a wake-up call. I do not know whether we would have answered the question differently. The only thing I would point out is that a lot of it has been around security practice; rather than necessarily something that is current in the software or anything else, there is an issue around security practice. The first thing is obviously for the Government to get their house in order and you will be aware, from the statements that have been made by Alistair Darling and Ruth Kelly, that there is quite a lot going on here. We have a report being done by PWC on HMRC. We have Richard Thomas and Mark Walport doing something around whether we need to look at the

Data Protection Act 1998. Gus O'Donnell has been asked by the Prime Minister to work with departments and I would say that in fact probably we will find that performance on this has improved. I know for a fact that in BERR in the last six months, there have been changes so that laptops and disks and things cannot be taken out unless they are encrypted. There is stuff going on in Government. I do not know about the exact timing, whether it was just after the report, but, with reference to the Information Commissioner, the Criminal Justice and Immigration Act has actually given him powers—I think it is since the report—to impose monetary penalties. In the process of going through the Regulatory Enforcement and Sanctions Bill, if there were illegal activity then we could give the Information Commissioner an Order that would give the ability to impose monetary fines which are actually unlimited, unless we limit them in the Order. The ICO has also since published guidance on how to notify companies about breach of security. We ourselves do have a business survey on information breaches which is interesting and we are very happy to send you that; I personally found it quite intriguing. There is quite a mixed picture, some improvements and some things that are still a little bit worrying but I was pleased that of IT spend, there is a trend of increasing spend on security, although still 20 per cent or thereabouts of companies only spend less than one per cent of their IT spend on security so there is clearly more that we could do. There is a lot going on. The fact that it is something that people are very aware of—that is on the front pages of the papers—has certainly meant that business as well as Government are taking this very seriously.

Q14 ***Lord Harris of Haringey:*** We recommended very specifically that the Information Commissioner be able to implement random audits of security measures. On 21 November Downing Street was briefed, after the HMRC incident, that the Government were taking this forward. What progress has actually been made?
Baroness Vadera: I am afraid I do not know the answer to that. I do not know whether Geoff knows, otherwise we will let you know in writing.
Mr Smith: That would be the best solution. I know that the Information Commissioner had been developing ideas around that and they have not been particularly well received, but that is not to mean that that is not going to happen. It may be that we might be waiting for the Thomas/Walport report which is going to be quite a fundamental look at the Data Protection Act, but yes, we will certainly write to you.

Q15 ***Lord Harris of Haringey:*** I am sure that would be helpful. You mentioned your survey on what is being done. In the report we recommended a data security breach notification law. The Government's response was that you "would consider whether we need to find more formal ways of ensuring that companies do—as a matter of routine—contact the ICO when problems arise. Government of course is now almost falling over itself to tell us when problems have arisen, even when data has been heavily encrypted. However, the number of communications from the private sector seems to be a trickle. I cannot believe they are immune to this sort of problem, and your survey suggests that will not be the case. What is the current thinking on a breach notification law?
Baroness Vadera: There is basically guidance that the ICO has since put out for the private sector that tells them about when and how they might consider—

Q16 ***Lord Harris of Haringey:*** That is guidance. Do you want to make it a compulsory requirement that people should notify those whose data is distributed generally?
Baroness Vadera: Your report and evidence that I read subsequently show that this is not straightforward, you want to find the balance between a tick box approach which makes people feel a little bit immune and actually some level of significance in the event. As you say, we are falling over ourselves to notify, as Government, every breach even when it is encrypted so we do have to find the balance. My personal view is that it is very hard and we are looking at all of this in terms of the various reviews that I have already mentioned, so I do not want to suggest something before we know what may come out of that. It would be very difficult to legislate or regulate for the level at which you should inform because it is really about proportionality and significance, is it not? All of this is being considered in the variety of reviews that are going on.

Q17 ***Lord Harris of Haringey:*** Health and safety legislation, by placing personal responsibility on individual managers and indeed on boards of directors, has transformed attitudes towards health and safety in the workplace. Is there not a case for equivalent legislation, as far as information security is concerned, to make sure that all managers and indeed all employees and indeed those who are responsible for organisations in both the public and private sectors, take this as their personal responsibility, with perhaps implications for their personal liability if they fail to do so?
Baroness Vadera: I do not personally believe that that would be a proportionate response, but, again, these are things that are being considered and looked at and I would not want to presume to speak before everybody has really considered all of the issues. All I would say about the health and safety regulations is that nobody said that anything is perfect and the

reason I know that is because we are reviewing those as well right now in my department. We need to have something that is proportionate and is going to be effective. The most important thing is being effective rather than just to say automatically that we need to legislate.

Q18 ***Chairman:*** Lord Harris's point does require underlining, that in the health and safety sector, major companies put policies in place and it transformed the statistics and the reality and that is worth putting on the record.
Baroness Vadera: I did have a statistic which I cannot remember off the top of my head, but actually quite a significant proportion of companies have security policies in place, as you will see from the survey.
Mr Smith: It is near 80 per cent.

Q19 ***Earl of Erroll:*** I just wanted very quickly to ask whether you do actually hold out much hope of being able to strengthen the powers even if you do alter the Data Protection Act when you consider what happened in the Criminal Justice and Immigration Bill when they watered down what was originally section 216 or 219 and introduced section 75, and then further watered it down so that the powers that were to be given to the ICO basically got watered down to a fine. There is no point in fining a government department, it will merely make the service worse, and as for fining an individual, well the person who has bribed them to release the information will probably offer to pay the civil penalty. So how are you going to strengthen it, if you are going to water down your provisions the whole time? It was not under parliamentary pressure either.
Baroness Vadera: Vernon knows more about that particular Act but on the Data Protection Act, we are still waiting for the recommendations so it would be slightly premature to talk about the fact that we are going to water down the recommendations before we have received the recommendations. That is not entirely fair.

Q20 ***Earl of Erroll:*** I am merely looking at the track record of what is just going through Parliament now.
Baroness Vadera: That may well be but we have not even seen what has been recommended. We are also attempting, through the Regulatory Enforcement and Sanctions Bill, to look at the imposition of proportionality in civil sanctions and fines and actually that would be something that we expect to see, not really in this sector, across the piece and that might give a very different overarching picture of what people expect us to do in terms of proportionality of fines relative to the damage that is caused.
Mr Coaker: It certainly would not be our intention to water down important legislation that we think is appropriate to deal with issues in this area. That is a statement that we would want to make this morning.

Q21 ***Lord Krebs:*** Just very briefly following up the question about voluntary notification of security breaches, if one is going down the voluntary route, I wondered whether the Government had any view about auditing of voluntary reporting. Presumably companies have internal audit mechanisms and is that something where the Government should be providing guidance on audit standards?
Baroness Vadera: Again, this was a part of the discussion around the ICO and we will come back to you on the fact that we understood that there was.
Mr Smith: I was trying to come back on Lord Harris's point which I think you are extending. Instead of looking at health and safety as an analogy, you could say that information is another business risk, information management is a business risk and should really be part of the corporate governance structure for risk management. I have to say I do not think it is quite taken in that way as much as it should be by corporate UK and possibly that is a line of policy development that we could think about. I am very nervous about Lord Harris's suggestion because we both lived through the Sarbanes-Oxley episode in the USA which was a knee-jerk reaction to the Enron scandal.

Q22 ***Lord Harris of Haringey:*** You get knee-jerk reactions when Government do not respond to a problem. If the Government responded proportionately at an early enough and appropriate stage, then you will not necessarily get that knee-jerk reaction.
Baroness Vadera: I do understand exactly what you are saying which is why, as you said, there was a statement made by Downing Street that we would be taking this forward. I have already outlined a number of views and we have given ICO extra powers, we do have guidance and we are monitoring the situation and it would be disproportionate at this point suddenly to say okay, therefore the answer is legislation.

Q23 ***Lord Harris of Haringey:*** A guide for boards of directors on information risk has just been produced as part of risk management and this might be something that the Department for Business might want to be picking up and encouraging boards to be taking very much more seriously.
Baroness Vadera: Quite a lot of recent events have shown that boards do not always understand complicated things about financial products or IT, so yes, that is certainly the case.

Q24 ***Lord Crickhowell:*** The Committee received evidence that there was no generally agreed definition of e-crime and no real data about how much was occurring, who was committing it, and what the trends were. Your response was that you were setting up a small high-level government industry working group, but there was "no need" for classification schemes "because prosecution should be based on the offence and not on the tools used". We have had a response from Nicholas Bohm of the Law Society's Electronic Law Committee, commenting (in his personal capacity) on your response and saying that it misses the point and that what e-crimes have in common is they require particular skills. It is all a very complex issue, they lack an ordinary location because they are often committed in large batches affecting victims in many different places at much the same time, they are international, the development by law enforcement bodies of the necessary skills and the effectiveness of their work and the priority it is given are all liable to be affected adversely by the lack of clear information about the incidents of e-crime and so on. How on earth can you effectively enforce if you do not have adequate data?

Mr Coaker: May I just start by saying thank you very much for the opportunity to come again to the Committee and may I just apologise to all the Committee if they felt that our response was over-defensive. I hope, in part with the answer that I give to Lord Crickhowell and to others, to be able to demonstrate the report that was produced by this Committee a few months ago now has actually helped drive the agenda forward and certainly the re-submission of evidence and the re-thinking that that has caused has also helped with respect to that. So may I apologise to all of you; it is no disrespect to the Committee or to any of the members. May I start with that point? If I can answer specifically what Lord Crickhowell has asked and then just say something about the way that we are thinking now to try to take forward some of these particular points. We have not set up a particular group, but let me come to what we are going to do. We have been working with a number of groups about what we should do with respect to the collection of data, how that should be measured, what would be the most appropriate and indeed effective way of doing that. We have been discussing this with a number of groups, not least the national e-crime strategy group, the CBI, Cabinet Office and others. Indeed we have also said that we will support the establishment of an industry-led partnership such as the Internet Crime and Disorder Reduction Partnership which my colleague Alun Michael has been doing an awful lot of work on through the UK Internet Governance Forum and we are very pleased to support that. In answering the point that Lord Crickhowell has made and in trying to come to an effective way of actually doing this, what we would like to develop, as part of the National Fraud Reporting Centre, is an integrated response to electronic crime. We know from the US IC3 centre that some 75 to 80 per cent[1] of crime on the Internet could be categorised as fraud, so we believe that that gives us an important starting point and indeed, IC3 has been advising us about how we might set up the National Fraud Reporting Centre. As a starting point, we believe that we would like to see all reports of fraud, much of which will be computer related, IT related, sent to the NFRC. One part of that work then, having done that, would be what we could reasonably expect to gather from individuals and businesses with respect to that, almost a one-stop shop for the reporting of fraud, much of which will be Internet related. I know we will come to "What about the bit of Internet crime that is not fraud?" and, again, NFRC could develop in a way in which that part, the 20 to 25 per cent, could go there as well[2]. Lord Crickhowell asks about the classification. It is fair to say that we would then expect, that information having been sent to the National Fraud Reporting Centre, to consider what categories that crime is falling into. Again, I was struck by the fact that if you look at the information we had from IC3 in 2007, at the data that they have had, you can see their top ten IC3 complaint categories. I think the point the Committee was making to us was that clearly, if you have that level of information being given to you and that information and those facts used then that can help inform the response, whether that should be what the individual should be doing to protect themselves, what the ISP should be doing to protect the consumer or indeed what Government should be doing or indeed what law enforcement should be doing, that level of information and statistical evidence can then be used. I hope that what I was saying was that we have listened to what the Committee have had to say. Whether or not people agree that the National Fraud Reporting Centre is the best vehicle by which that should be done, what we do not want is a multiplicity of National Fraud Reporting Centre, eCrime Reporting Centre and so on. We are just trying to find a way of sensibly bringing all of this together. I hope that goes some way to reassuring Lord Crickhowell that we use that to collect the evidence and then to look at how we define that.

Q25 ***Lord Crickhowell:*** Well I certainly agree that that response was a great deal more positive and constructive than the original response to the Committee. I am a bit worried that that answer and a number of previous answers involve you saying "Well, there is a lot of talk going on and we are having a lot of discussion and a lot of consideration".

[1] It is based on IC3 Annual Report

[2] This would be in the longer term.

In the meantime, of course, the volume of computer crime internationally is rising, all the evidence is that it is rising sharply and it does seem to me that it is pretty urgent that some of these things are brought to a positive conclusion. You say a lot of the kind of information we felt was necessary will be emerging, but if you do not have some fairly clear classification of what you want when the process is ended, it does seem to me that there will be a bit of a lacuna in what we need. May I say that I think most people on this Committee would hope that all these discussions are going to come to some positive answers fairly quickly because the need is urgent? I suspect, if they do not, the Committee will want to return and ask why not quite soon. I suppose as a Welshman I am bound to ask another question which has been drafted here about the evidence from Team Cymru who gave figures for credit card trading on the underground economy, dedicated Internet Relay Chat, IRC servers, where the criminals sell data about credit cards and bank accounts to the people who know how to cash them. Have government officials met Team Cymru? Have they obtained any more information on the evidence? Do you in fact track the chatter between the criminals that goes on on the Internet to see whether there are things that need following up by government departments?
Mr Coaker: I should have introduced Justin Millar who is one of the officials that deal with this. First of all, may I answer the specific point that Lord Crickhowell made with respect to his Welsh interest. The important point he has made is a really important point. It is a fair comment to make that there is a sense of urgency now in this and that is what I was trying to say at the beginning about the injection of pace, momentum and desire to change that has now been created by what the Committee has done. To reassure for Lord Crickhowell, we have now established an inter-ministerial group on fraud and I preface that with the caveat that we do know that a large amount of computer related crime is fraud. We have set up an inter-ministerial group which includes ministers from a wide variety of departments. At the first meeting, we did say that there was a need to look at the issue of computer-related enabled fraud and indeed there is a draft paper which is available for the next meeting, which will take place before the recess about how we take all of this forward. I will not move on to the other questions which will make other points about some of the other issues that I know the Committee had concerns about, but this document and the letter I have had from the Attorney General about the need for urgency and will give us the speed with which we need to act. I do not know the specific case to which Lord Crickhowell is referring, but just to say that we are all ensuring, partly in developing our work through the National Fraud Reporting Centre, that we will be speaking to people in the private sector and indeed in the devolved administrations, et cetera, so there will be lot of work going on.
Mr Millar: I am aware of Team Cymru, but we have not met them.
Mr Coaker: Perhaps we ought to.

Q26 ***Lord Crickhowell:*** As you were given advance warning that we were going to ask the question, it might have been wise for at least someone to pick up the phone and talk to them.
Mr Coaker: I apologise if we did not. I had not realised that question was going to be asked.

Q27 ***Chairman:*** There is no reason you should have known that this question was going to come up but in fact, they did provide evidence for us that has been published.
Mr Coaker: Well I apologise for that; we will look into that and certainly we will meet with them.

Q28 ***Lord Harris of Haringey:*** I am not sure they have much connection with Wales.
Mr Coaker: Yes, they are based in the States. Anyway the serious point is that it is a point well made and we will look into that of course.

Q29 ***Earl of Northesk:*** Let alone the classification of e-crime, is there not an additional problem here, namely that the available resources and expertise, for example within law enforcement, just are not there either? I have two points to make on this, one of which is that the absorption, for example, of the National Hi-tech Crime Unit into SOCA then completely destroyed any IT focus in terms of investigation, so far as I can tell. There is another issue here which I find absolutely fascinating, which is the knotty problem of Phorm. A number of aggrieved subscribers think that an offence has been committed with their particular Internet services purely and simply because BT conducted trials secretly. However, I happen to know that a number of these aggrieved subscribers have hawked themselves around, Home Office, the Information Commissioner, law enforcement, and been given the brush-off time and time again. What are the Government actually going to do in terms of providing the relevant resources and expertise out there so that action can actually be taken against e-crime?
Mr Coaker: May I ask whether we have moved on to the issue of the funding for the e-crime unit?

Q30 ***Chairman:*** Yes, and the Earl of Erroll will be picking that up as well. If you want to answer briefly and then we will explore the issue of funding afterwards.

Mr Coaker: I may have some interesting things to say in the next answer with respect to law enforcement, so may I answer your question together with the Earl of Erroll's question, if that is okay with you?

Q31 ***Earl of Erroll:*** A quick rider before I start. The first thing I was going to say was that I did not feel there was disrespect in the response from the Government at all. I rather felt that there were probably problems of budget and a feeling of how were you going to get it out of the Treasury, therefore the usual thing was to say "Well, let's talk about it a bit more and then hope that something appears in the next budget round" or something like that, which was disappointing. I think what the Earl of Northesk was asking was slightly different from what I am about to ask which was that he was thinking about how this was classified and whether Phorm is a crime or is not. There are rules that would suggest that it is but no government department wants to pick it up and say that it is. Everyone wants to shift the buck and that is very different from what I am about to ask actually, which is specifically about the funding for the Police Central e-Crime Unit which I believe will now be called the National e-Crime Unit and I believe it is something which is happening finally. It did strike me that we recommended that necessary funds should be made available to this, because it is all very well having all your fraud reporting and the National Fraud Reporting Centre, but if you do not go out and chase a few people and lock them up, there is nothing to de-motivate future criminals; you know all about them but you are doing nothing about them. SOCA is tasked at serious and organised crime level and with an international flavour, so they will not touch internal e-crime and e-fraud. We were wondering where you have got to in your thinking of funding a unit which can produce some coordination, produce a central law enforcement unit and is very much about enforcement, not reporting, which could work with your National Fraud Reporting Centre into which you are about to pump £45 million, or something?
Mr Coaker: Fifteen million.

Q32 ***Earl of Erroll:*** Why could you not find a little bit less money to go and actually arrest some criminals?
Mr Coaker: First of all, may I say that we have received, as the evidence shows, the business case from the Association of Chief of Police Officers and you received their evidence and you know about that. Certainly that has been one of the questions that I have continually been asking. The answer to Lord Crickhowell is that I think it is a step forward and I was grateful for the comment about it being more positive, about reporting to the National Fraud Reporting Centre. However, the question really is, if all these reports of fraud or computer related crime are going to the National Fraud Reporting Centre, the famous "So what?" question, is it not? What happens then as a result of all of that? Just to put a bit of context on this, if it is okay with the Committee, it seems to me that in asking that question that also begs other questions around the fact that we have the SOCA e-Crime Unit, we have CEOP dealing with issues of child abuse, which we would not want, in any shape or form, to change because it has actually been very, very successful and I am sure we would all agree with that.

Q33 ***Earl of Erroll:*** Entirely.
Mr Coaker: Absolutely. Then we have other police forces conducting their own local investigations and sometimes the Met with its own unit and so on. So you have different pieces of law enforcement doing different things, but there is a gap without a shadow of a doubt. Again, as part of the work that was done under the new inter-ministerial group, which has only met once but has actually transformed the landscape, we asked how to take this forward. What we need is the National Fraud Reporting Centre developing in the way that I have said, but alongside that a law enforcement capability. We have been working very hard with the police, other law enforcement, with industry, with some of my colleagues, both in the Lords and in the Commons on all of this to try to take this all forward. What I did not want to happen was for the National Fraud Reporting Centre to set up a law enforcement arm which did not relate to all of these other bodies. Although it would in the first few weeks gain plaudits and people cheering saying what a wonderful thing it was that the Government were finally funding an e-crime unit, without that structure, without that context, without that sense of how that relates to all of the other things that were going on, that would have been difficult. Just for the information of the Committee, I am actually meeting with law enforcement agencies, with the City of London Police, who I should have mentioned have a lead force role with respect to fraud, with the Metropolitan Police and with SOCA and with others on 4 June to discuss this. Alongside that, is the issue of funding and what we say in the Home Office is that within reason—I have to put the caveat "within reason" because we have no budget figure for this piece of work, although I know we have a budget figure for the piece of work that went before with respect to the ACPO e-crime unit, the police e-crime unit—within reason the Home Office will look to fund that law enforcement capability alongside the National Fraud Reporting Centre. What we are trying to achieve, and what is hopefully more positive, is somewhere fraud is reported to and a lot of work to be done with that and then alongside that a law enforcement agency. My final point on this is that the key question that then needs to be worked

out—and I notice the ACPO lead, Janet Williams, has made this point on a number of occasions—is what you do at a national level, then what you do at a regional level and then what the local police do and how all of that relates to each other and inter-relates so that we get national strategic law enforcement acting as a catalyst for change, it seems to me, and then working down to see how that works with organised crime at regional level but also at a local level where we know, because all of us we live in communities where people, who in the great scheme of things have not lost millions of pounds but have lost a few pounds which are immensely important to them and the lack of confidence that they then have about using the Internet. We are at the beginning of those sorts of changes and I do not want to promise jam tomorrow but there is real work going on now which will bring about that change.

Q34 ***Earl of Erroll:*** Is this not rather a matter of urgency because, for instance, there was a recent DDoS attack which hit 104 companies and only one got around to reporting it to the police because of course they knew nothing was going to happen. If you get this National Fraud Reporting Centre website going or somewhere they can report it, it is going to rocket. If you do not have some capability in place to deal with it, you are just going to get overwhelmed; you are going to add to the backlog. You used to have a huge amount of expertise there in the NHTCU which got very efficiently removed into SOCA to kill it and I am not quite sure why. Could you not have drawn on some of that experience? They knew a lot about how they were doing and beginning to coordinate things across police forces. If you do not get started soon, we are going to get overwhelmed.
Mr Coaker: Again, in answers I made earlier to Lord Crickhowell, there is a sense that there is a need to act as quickly as possible on this, that is why, in terms of trying to draw together all of the expertise, SOCA of course, where the National Hi-Tech Crime Unit went to, will be at this meeting and why the ACPO lead will be at this meeting.

Q35 ***Earl of Erroll:*** There are only five originals left.
Mr Coaker: I appreciate that point; I cannot go back to where it was. What I am trying to reassure you is that obviously we want to listen to what all of the various law enforcement people say, what the experts say about how we do this and, to repeat myself, about what it means nationally, regionally and locally.

Q36 ***Earl of Erroll:*** Very briefly, could you also look, because I remember Commander Sue Wilkinson thinking what we saw on our visit to the United States was an extremely good idea, at the network of centrally-funded computer forensic laboratories, because you are going to need that support as well when you get going and if you do not start setting these up, you are going to run out of time. Your report said you were considering an infrastructure, so are you looking at these sorts of things as well?
Mr Coaker: As part of all of this work, we are indeed looking at all of this as part of that piece of work. What I am trying to say is that we have moved considerably on from where we were before, where in a sense there was a discussion about what law enforcement made, to accept the Committee's recommendation that there needs to be a formal law enforcement response to that. What I cannot say to you, because the detail is not worked out yet, is exactly what that means, but I agree absolutely with the need for urgency, absolutely with the need for intelligence and, alongside the National Fraud Reporting Centre, it is our intention to have a National Fraud Intelligence Bureau which develops the intelligence and then see how that information can be transformed into work packages of information, how that can be transferred, whether it be at a national level, at a regional level or at a local level, into effective law enforcement which will make a difference to the organised criminals at the top but also give confidence to those people at the bottom that their crime which, in the greater scheme of things, may not be a great loss to the country as a whole but to that individual is a huge loss.

Q37 ***Earl of Erroll:*** It may not appear to be a great crime because you are looking at the individual end, actually the same person may be perpetrating it using the Internet and then going back a thousand times so they are actually ripping off £1 million.
Mr Coaker: I was only trying to say that so-called small crime is important as well as the big crimes.

Q38 ***Lord Warner:*** We have been round the track before in other areas like this, football hooliganism, animal rights activists, child pornography and the wheels of ACPO do tend to grind exceedingly slow sometimes when a key problem is identified which does not fit well into 40 or so police forces. It just does not fit well and there is a very good strong record of ACPO holding out for more Home Office money before they actually tackle some of these issues. You know it, I know it, the Committee knows it. What guarantees do we have that this is actually going to be taken seriously by ACPO and the kind of ceding of local force sovereignty that is required to make this really happen is actually going to happen? The past has not been reassuring in that particular area.
Mr Coaker: That is an extremely good question. The reason it is a good question is because, if you gave it £5 million, it would solve the problem, if you gave it £10 million, you would double-solve the problem. Of course, there is always an issue of resources, but there

is always an issue of how those resources are used. Let me just say to Lord Warner why I think that ACPO will move on this. They have been very supportive in helping us develop our work in this area. They have been very involved and I have been very grateful for their involvement in the development of our thinking around the National Fraud Reporting Centre. Why I particularly agree is, that Janet Williams is the ACPO lead now with respect to this who is saying that it is not only about money, it is also about how this is all organised. She is the one who is saying again and again and again how important it is that, of course, you have a national unit which acts as the strategic body and which is the catalyst for change, which organises that, but if you then do not link that in to what is happening, if you take the regional intelligence units at regional level but also that individually the forces do not respond, then she is saying that we will not have the change in capability or indeed bring about that step change that we all want. That is what gives me confidence in it because, when she discusses with us about this, she does not only talk about money. She does not only say if only she had the money she could deal with it. She says that it is about bringing about a change; of course we need resources but there is a cultural change which is needed as well and organisationally we need to deal with that and that is what gives me the confidence in this work.

Q39 ***Chairman:*** Is not one of the issues here that, as you keep saying, properly, there is a national, there is a regional and there is a local but of course this kind of crime does not break down in that way? There is not the same attachment to a location; where the individual loses money they have a bank account and live in a house and equally there is someone who is taking that money, who lives somewhere else, but the structure of the crime is really radically different and therefore radical thought is required.
Mr Coaker: That is an important point. I suppose part of what I am thinking as well though is and, again, the next question deals partly with that, is trying to give local people a confidence that if they live in 14 Derry Street, Sunderland, if they talk to their local police although they may not be the appropriate first place to go, the local police will have some understanding of how to deal with that, where that should go and what the appropriate response is and that is the key organisational change in pattern that we need to build.

Q40 ***Earl of Erroll:*** Two things, very quickly. The first one is slightly linked with both sides of this, which is that one of the things is where people go for advice on these things and this is part of this whole thing and the Government have been very vocal about backing *Get Safe Online*. The interesting thing is that I was talking to PayPal the other day and they feel that the Government are not putting their money where their mouth is and business and industry would like to have a definite lead, somewhere that they could all get in behind and do it. Do we see *Get Safe Online* as being that thing in the future?
Mr Coaker: Yes, we do see *Get Safe Online* as a key vehicle to develop this and the Cabinet Office are responsible for much of the information about that. Part of this is trying to get that information out there and the Cabinet Office are on this inter-ministerial group, there is a whole new emphasis on getting the information out there. What we are saying has been said before: of course ISPs have a responsibility, of course Government have a responsibility, of course law enforcement has a responsibility, but also we want, in the same way as we teach somebody the Highway Code in order to help them cross the road safely but we have road police and we have traffic lights and so on, to make the same analogy to the Internet. You have to have all those other things but you also have to tell people to take responsibility for themselves. In order to do that, which is the point PayPal and others are making, they need that information given to them in a way which they can understand.

Q41 ***Earl of Erroll:*** The point they were making was they wanted a clear lead from Government as to what they should be getting behind and you need to be able to get together with industry and decide which one you are going to back, whether it is that one or another one.
Mr Coaker: Get Safe Online is the one that the Government are currently backing.

Q42 ***Earl of Erroll:*** In which case, you need to get the funding sorted out and talk to industry about it.
Mr Coaker: Fine and we will do.

Q43 ***Earl of Erroll:*** The next thing is about frauds being reported to banks rather than to the police. We were quite worried about this because we felt that frauds should be reported to the police first and they should then filter out what goes to SOCA, what goes to banks, according to who is best capable or to the National eCrime Unit, whoever is best able to deal with it. Apparently an investigation by the BBC last June showed dramatic falls in the amount of fraud being investigated by the police. This change of reporting it to the banks first was to try to make it all more efficient and less police bureaucracy but have you actually changed the system for the better? Is there an increase in banking fraud being investigated by the police or has it all just been swept under the table?

Mr Coaker: Let me say the positive thing first. We are trying to engage with the Committee because of the feeling the Committee had that we had not properly engaged in some respects with some of the points that were made before. I know the Committee was unhappy about this particular matter. It was done because the Government believed, with the Association of Chief Police Officers and the banks themselves, that actually the system before was not particularly working either. These figures are probably available but in the last figures you have before the new system came in, in April 2007 59,000 recorded crimes with respect to fraud, cheque and plastic card crimes were recorded by the police; 59,000. That has been dropping dramatically over the last few years; it is not a sudden thing but it has been consistently dropping over a number of years. We wanted to see whether there was a better way because we were worried about this reporting of fraud, that perhaps it was not being reported. So it was an attempt to put in place a system whereby people would go to the banks, report that first, the banks would get a better overview of what was happening and then report that to the police. In the first instance this would reimburse the individual who had lost money through no fault of their own, but, secondly, we thought that the bigger overall picture might actually help with respect to the investigation of the crime. The Committee asked us to review this. I know that some of the professionals that you had evidence from have said that they have received a lot of reports. All I can say to you is that we have not, from the police or banks, although you might say that is inevitable, or individuals, we have not had a lot, if any, problems raised about this, but we will have a look at it. I know the Committee asked if we would review it and see whether it was working in the way that we intended, so we will have a look at it. I am not saying we will change it, but it is reasonable to say that we will review it. In terms of the investigation, we do not collect the statistics on the levels of investigation that are being conducted by the police with respect to this, so I cannot talk to you about that and of course we do not have not the 2007–08 crime figures yet; they are not published until July.

Q44 ***Earl of Erroll:*** One of the things that really worried us as well though was where the liability lay. We do know from some stuff from the Financial Ombudsman Service, that the banks are trying not to pay out in certain circumstances. This is not so much to do with online fraud but saying that the chip and pin system in inviolable and absolutely totally secure. We also know that the Financial Ombudsman Service does not really have the expertise to adjudicate in this and yet is being held to be correct. No-one yet has had the money to take a case to the courts so it is tested properly. This is not in your briefing at all.

Mr Coaker: It is the banking code; I know what it is.

Q45 ***Earl of Erroll:*** There is some stuff going on in there which at some point is going to hit the press and is going to hit things because the banks do try initially to offload liability and they have a history of doing this. They did it when the first ATMs appeared with pin numbers; they are now doing it with chip and pin which, because of the fallback mechanisms and the magstripe, there are weaknesses in it which they are not admitting and they are not actually showing true technical evidence to the Financial Ombudsman Service, who do not have the technical expertise to adjudicate. One of the things we recommended was that liability should be passed, rather as in the old Bills of Exchange Act, back onto the banks, not for things which are clearly fraudulent instructions, but where the token used is inadequate. In other words, trying to do electronic transactions, with the sort of security they have, is inadequate. If the liability went back onto the banks, they would then have the financial incentive to issue a more secure two-way, two-channel authenticated token and that would reduce fraud considerably. This clearly will not be popular with the banks because it will involve extra cost. What is your feeling about this?

Mr Coaker: I know that, with respect to the liability, the banking code says that if people have not acted fraudulently, then the banks will reimburse them for the money that they have lost, and I know the issue then is that the banks are saying that individuals were negligent in what they did, therefore they lose. Then people take it to the Financial Ombudsman Service and my understanding is that the Financial Ombudsman Service has not found the banks to be acting inappropriately and people say there is something wrong with the Financial Services Ombudsman. I cannot say that, I am not an expert with respect to the Financial Services Ombudsman but it seems to me that the ombudsman system works extremely well. No doubt, this debate will continue.

Q46 ***Earl of Erroll:*** The way round it is being done at the moment is that the person who has lost the money has to prove that the bank system did not work. The problem is that the banks are the people who have the information to say whether it worked or not and they are not releasing the correct information for that to be proven. It needs to be run through the courts.

Mr Coaker: I do not know. Online banking fraud has fallen; the issue now with banks is where the card is not present, that is where the big increase in problems has come.

Q47 ***Earl of Erroll:*** If you put the liability onto the bank, we were suggesting that they would issue a better token.
Mr Coaker: That is part of the debate that has been ongoing. If you make the business liable, we might see an improvement. One of the things I was going to say earlier on is that, with these things, the Government try very hard to move through self-regulation and we have seen a lot of progress in other areas. I have had a lot to do with child protection and that has worked fairly well and that is the path that we have chosen to take.
Baroness Vadera: I would be very happy to talk to the Financial Ombudsman Service about any issues that they might have. My understanding of this, and the way I would come to it is that the banks already do feel liable via the banking codes. It is not that they believe that they are not liable and all that a piece of legislation would do would actually be to say that they are. They do behave like they already are and they believe that they already are. The issue comes around the area of attribution of whose fault it was where there is a grey area and I am in the middle not sure that the piece of legislation would actually be able to define that so that actually it would necessarily change that. It might be that therefore we need to make the Financial Ombudsman Service better able to decipher that or get through the greater powers of the bank to pass it on. I am not sure the legislation would change that balance of power.

Q48 ***Earl of Northesk:*** You recommended that you ratify the Convention on Cyber Crime, signed back in November 2001. The Government's response was that this would happen as soon as possible and that there would be Computer Misuse Act changes in April of this year. However these changes have not occurred. Why is that and what is causing the delay?
Mr Coaker: There has been some delay but I can say to the Committee that we will enact the various pieces of domestic legislation that need to be enacted in October this year and we will ratify, unless something dramatic goes wrong. I can say to the Committee that we do intend to ratify by the end of this year.

Q49 ***Earl of Northesk:*** We also recommended that you should review mutual legal assistance procedures and the Government's response was that provisions within UK law for this were sufficient. Much of the evidence the Committee received, stressed how slow other countries were at providing assistance, which would seem to argue in favour of the review. The Met Police recently told us that almost all Internet investigations have an international dimension. They also wanted to see a comprehensive review of the process. Do you have any firm plans to address the police's concerns?
Mr Coaker: I will ask Justin to talk to the detail of it. May I just make the general point that whilst we have talked about how, with respect to computer-related crime, to distinguish between national, regional and local, the international dimension to this will become increasingly important, about how we work with other agencies across the rest of Europe but across the globe as well. This will become of increasing importance which is why ratifying the convention is extremely important but there is a lot more that we need to do across the globe almost to tackle this issue.
Mr Millar: Very briefly, the G8 hi-tech crime sub-group is looking at this issue and I believe the Council of Europe Convention group are looking at things like the 24/7 networks, to see how their efficiency can be improved. There is also some work going on bilaterally between the UK and some other countries. Obviously those may not be the countries with which we necessarily have the greatest time lag in gathering evidence. However, there is work ongoing to look at improving the efficiency of the information transfer.

Q50 ***Chairman:*** May I thank you very much indeed? It has been a very helpful session.
Mr Coaker: Could I please make one point? I was very struck by what the Committee has said about urgency. Perhaps it would be helpful if every couple of months I dropped a note on what is happening in this inter-ministerial group and the progress that has been made, if that would be helpful to the Committee, on some of the points that have been made. I am quite happy to do that.

Q51 ***Chairman:*** That would be exceptionally helpful. We are increasingly keeping a watching brief on what happens to our reports and for your response to be proactive rather than reactive would be very much what we had hoped for. We thank you for the way in which you have responded and taken on board what were some very serious issues. May I just refer in passing to the issue of negligence? That is a difficult one to define because of the complexity, but, on the other hand, there is responsibility and it is where responsibility lies that is driving quite a lot of our thinking in fact. Lastly, you refer to the events of the last few months as a wakeup call. We like to think of our reports as, from time to time, a wakeup call.
Mr Coaker: It has been that.
Baroness Vadera: It has been that.
Chairman: I just put that one on the record. If there are any further clarifications, you will receive a record, a transcript of the meeting or if there are points that came up where you feel it would be useful to give us a note, that would be very helpful and will be part of the formal proceedings of the Committee.

Supplementary memorandum by Baroness Vadera

When Vernon Coaker and I appeared before your Committee on 20 May, I promised to write to clarify where things stood on the idea that the Information Commissioner should be permitted to conduct random audits of the data protection arrangements in companies. I have consulted colleagues in the Ministry of Justice and I have taken the opportunity to address again the key developments in data protection that were covered in our discussions in the House.

The Prime Minister asked the Information Commissioner to carry out spot checks of the compliance by Central Government Departments with the Data Protection Act on 21 November 2007. The Ministry of Justice is working with the Information Commissioner to finalise the arrangements of these audits which will start shortly.

On 17 December 2007 the Sir Gus O'Donnell Review published *Data Handling Procedures in Government: Interim Progress Report,* which set out the findings of the review so far and provided an update of the progress. In particular, the Review indicated that legislative steps should be taken to enhance the ability of the Information Commissioner to provide external scrutiny of arrangements by considering the options to extend the spot checks of Government Departments to the entire public sector. The Thomas/Walport review is also considering this issue and will make recommendations regarding the Commissioner's audit powers when it reports in the first half of 2008.

The Sir Gus O'Donnell review on Data Handling is also due to report in final form shortly, as are the Kieran Poynter and Edmund Burton reviews. The Government will take a considered view on what further measures it needs to take to strengthen the protection of personal data in light of the recommendations of these and the Thomas/Walport reviews.

I recall that there was critical comment when we met on the new power of the Information Commissioner to impose a monetary penalty for serious contraventions of the data protection principles. My Ministerial colleagues have asked me to assure you that the amendment was the result of well-considered research to ensure not only the most effective form of sanction, but also that any new powers of the Information Commissioner should align with Government measures to make regulation across the board more effective and efficient.

In addition to this, the Government has brought forward a power to amend by order the penalty for those found guilty of unlawfully obtaining, procuring or, disclosing personal data to a custodial sentence. We believe that this gives a strong signal that the lucrative and illegal trade in personal data will not be tolerated and that there is a stronger deterrent available if this activity continues.

Can I also take this opportunity to thank the Committee for the positive discussion when I gave evidence. I am sure it was clear that I was coming new to this subject area and I hope you now appreciate that there was no intention to deliberately undervalue your Committee's work. I found it a stimulating report and—while there may still be differences between us on the best solutions—I think we can agree on the need to make progress in many of the areas you have identified in your Report and I hope we can work together. My offer to maintain a dialogue on this subject was made in this spirit.

I am copying this letter to Vernon Coaker at the Home Office and to Michael Wills at the Ministry of Justice.

3 June 2008

Written Evidence

Memorandum by Professor Ross Anderson

Colleagues and I supported your report's recommendations and found the Government's response to be deeply disappointing. I would like, however, to add a few points of detail.

First, during the last quarter of 2007, three colleagues and I wrote a report for the European Network and Information Security Agency entitled "Security Economics and the Internal Market" which I incorporate herein by reference. (It may be accessed from their website or from mine.) This report was based on intensive study of the available statistics relating to online crime and security, coupled with extensive consultation with stakeholders to determine what policy options were helpful and practical. It also built on your committee's work.

We came up with 15 recommendations for action by the European Commission, and these push very much in the same direction as your committee's findings. I would like to suggest that committee members read at least the first six pages of our report, which summarises our work. Among other things, we recommend a comprehensive security-breach disclosure law, the collection of better statistics on online fraud and crime, the better alignment of incentives through liability, and standards for network-connected equipment to be secure by default. There are some differences of detail, because of our study's different scope and audience, but no substantive points of conflict.

Second, we remain unimpressed by Government efforts on information security, and hope that the complacency expressed in its response of October 2007 has been shaken by the HM Revenue & Customs (HMRC) scandal. The problem is of course many-faceted, involving a wide range of government functions from operations through regulation to enforcement.

On the research funding side, I note that the National Science Foundation (NSF) is allocating a nine-figure sum to the Global Environment for Network Innovations (GENI) project, whose aim is to develop options for a next-generation Internet that would give security and quality-of-service guarantees; I see nothing comparable from the UK funding agencies.

On consumer protection, the government is being disingenuous in claiming that the banking industry's practices provide adequate protection. I would like to point you to a submission that Foundation for Information Policy Research (FIPR) colleagues and I made to the Hunt Review of the Financial Ombudsman Service, in which we show the contrary.[1] The banking code also provides scant protection; where a password or PIN has been used, the bank often simply claims that the customer must have been negligent or complicit. Given the large variety of technical means by which passwords and PINs can be harvested without customers being aware, this argument is very shaky—yet the Ombudsman routinely backs the banks against customers who complain, and customers have little effective redress in the courts because of the rules on costs and because of their lack of access to technical information and expertise. Dozens of victims approach me every year out of desperation, because of my research papers on card security; I'd estimate that between 1,000 and 10,000 people each year are denied compensation after being the victims of third-party fraud (what's more, these victims are overwhelmingly poor, female or black. I can't recall a middle-class white man coming to me with a tale of woe).

It is also noteworthy that the Treasury lobbied alongside the Association for Payment Clearing Services (APACS) and Barclays to get the European Union to restrict consumer protection in last year's Payment Services Directive. The Government has not been a passive observer of this tussle but has actively helped the banking industry to decrease their own liability at their customers' expense. In this context, it is somewhat breathtaking for the Government to say that "*Imposing legislation on banks to be held liable for losses incurred as a result of electronic fraud does not seem to be the appropriate approach in ensuring that banks maintain their customer information securely*". Such legislation exists in the USA (Regulation E) and has had precisely that effect.

On the question of kitemarks, we recommended to the European Network and Information Security Agency (ENISA) that their scope should extend to all network-connected equipment. As computing becomes pervasive, large numbers of devices that at present have at most standalone computing capability will be online. Thus, in future, the spammers and phishermen might not be building their botnets out of PCs but rather out of network-attached TVs, air conditioners or even cars. Internet service providers and others who

[1] www.fipr.org

suffer financial losses should clearly be able to recover them from negligent vendors, else the vendors will have insufficient incentive to engineer their products properly. Our proposal was that vendors should have to certify that their products were secure by default—and where this turned out to be untrue, they would be liable for damages. This seems to be a minimal, light-touch way to align incentives.

Finally, your last recommendation was on guidance to the judicial system about the dangers of relying on unsupported credit and debit card evidence. Last month, a "Newsnight" investigation described the case of Jane Badger who was prosecuted for attempted fraud after complaining of phantom withdrawals from her account with Egg. The prosecution collapsed once the defence obtained expert help and the right questions were asked. It's not just the policy folks who need to catch up with the technology of electronic crime, but police and prosecutors too. So I urge you to keep on pushing for better court guidance and judicial education.

19 March 2008

Memorandum by the Association for Payment Clearing Services (APACS)

Our input consists of our reaction to HM Government's response highlighting the areas of greatest concern to APACS and its members, and our suggestions to help guide the Committee's future deliberations.

APACS Comment on HM Government's Response

1. *"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 the recording of all forms of e-crime".*

The Government is correct in saying that crimes committed by computer are "standard offences facilitated by new technology" this does not mitigate the need for developing greater understanding. The correct measurement of crime is an important step in the process of understanding the impact of certain types of criminality, and from there to understanding how to define and allocate the resources required to tackle them. In the case of e-crime, there are a range of techniques and skills used by criminals that are highly specialised and that therefore require a specialised response. If the Government is not in a good position to understand the nature of the crimes being committed, then it follows that it won't be in a good position to understand how to direct law enforcement and the courts accordingly, or to develop appropriate legislation. We therefore encourage the Committee to focus on helping to create the conditions for policy makers to better understand the impact of e-crime.

2. *"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. We urge the Crown Prosecution Service to publish the guidance as soon as possible, so as to avoid undermining such research in the interim".*

We are broadly supportive of the Government's response to this recommendation. However, we would add that the UK lacks and continues to lack a Computer Emergency Response Team (CERT) that is capable—in terms of skilled resource and mandate—of assisting in the fight against e-crime, and that we consider this to be a serious shortcoming. We would urge the Committee to examine in depth the leading global exemplars of such CERTs, namely AusCERT in Australia, CERT/CC in the USA and CERT.BR in Brazil. These three in particular have developed far-reaching capabilities that have proved of enormous value in the fight against e-crime. It continues to frustrate practitioners and security experts in the UK that we have no direct equivalent, and we believe that its continued lack has contributed to the UK suffering disproportionately from e-crime.

3. *"We recommend that the Research Councils continue to give such fundamental research priority".*

We have no comment on the Government's response.

4. *"It is time for the Government to develop a more holistic understanding of the distributed responsibility for personal internet security".*

We understood the spirit of the Committee's recommendation to be, that the Government should take a more active role in understanding what various public and private sector stakeholders can do to help maintain personal internet security, and that it should work proactively to ensure that these responsibilities are being upheld. In this APACS strongly supports the Committee's recommendation and we would argue that acceptance of it as a principle by the government would greatly assist in supporting many of Committee's other recommendations.

5. *"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 on obligation will be placed on ISPs to provide a good standard of security as part of their regulated service. We recommend that the ISPs should be encouraged as part of the Kite mark scheme to monitor and detect "bad" ongoing traffic from their customers".*

As banking customers increasingly shift more of their transactional and banking activity online, they become increasingly reliant on the security of services offered by ISPs. APACS is supportive of moves to encourage ISPs to improve the level of security that they offer to their customers, and to take a more proactive stance to identify and prevent "bad" traffic from their customers. We believe that these developments are best left to industry and competition to provide, but we also believe that the Government has a strong role to play in promoting the principle of a safer internet, and the specific steps needed to achieve it.

There are a number of self-regulatory approaches that could serve as examples for working further on this recommendation, ie The Banking Code. The 2008 edition of the Code enshrines a guarantee that online banking customers will not be liable for any losses if they are the innocent victim of fraud.

6. *"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".*

Revocation of mere conduit, even on a selective basis, is likely to be an enormously complex challenge, but one that we believe could yield positive benefits if done with sensitivity. Whilst the Government is correct to say that many ISPs do take proactive steps against customers whose machines are sending out spam or infected code, many more either do so with varying degrees of effectiveness or not at all. Indeed one could argue that the current data on this speaks for itself. For example, the UK is a leading source of botnet-infected computers, and UK bank brands are regularly amongst the most heavily targeted by phishing gangs. By offering clarity on the extent of mere conduit provisions, ISPs would be in a better position to understand their areas of responsibility, and the market would be provided with a higher baseline of response from ISPs.

7. *"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".*

We have no comment on Government's response.

8. *"We recommend that the Government explore, at European level, the introduction of the principle of vendor liability with the IT industry".*

We have no comment on the Government's response.

9. *"The steps being currently undertaken by many businesses trading over the internet to protect their customers' 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 a position to prescribe the security precautions that should be taken; however, they do have responsibility to ensure that the right incentives are in place to persuade businesses to take the necessary steps to act proportionately to protect data".*

We are broadly supportive of the Government's response to this recommendation. We do not accept that the financial services sector "*refuses to accept responsibility for the security of personal information*". The financial services sector responsibilities in this area are very clear and at all times individual institutions lay these out in their communications with customers and overall account terms and conditions. For example, section 11 of The Banking Code sets our subscribers' responsibilities in respect of personal customer information.

The financial services sector takes the security of our customers' data extremely seriously and it would be true to say that our success in maintaining an appropriate level of security is demonstrated by the high and growing level of online banking usage.

APACS members and the wider banking community, have also been instrumental in driving the implementation of a number of initiatives designed to greatly strengthen arrangements for the protection of customer data. For example, the Payment Card Industry Data Security Standards (PCI/DSS) are intended to protect sensitive customer data that may be held by merchants and others engaged in accepting and processing face to face and remote card payments. PCI/DSS is being implemented on a global basis and represents one of the most significant developments to protect customer data yet seen.

In the specific field of online banking fraud, banks have taken aggressive steps to identify and remove sensitive customer information from the Internet, for example, in the form of log files generated by malicious spyware that has infected customer PCs. However their efforts are often hampered by ineffective or obstructive local legislation in many countries. For example, under the law of a number of countries including several US states,

data on compromised customers gathered by spyware or phishing sites, and located on an open web server, is considered to be the property of the criminal and obtaining or deleting the data may itself be considered a crime. This astonishing state of affairs means that there are occasions where enormous obstacles are placed in front of those committed to fighting this type of crime.

We would wish to see the Government taking steps to ensure that law enforcement is able to swiftly and effectively demand the removal of sensitive personal data from online sites, and that the Government takes a leading role in promoting this stance on a global basis to ensure that criminals have no place to hide.

10. *"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".*

We are broadly supportive of the Government's response, and feel that the Committee have misapprehended the nature of existing arrangements to protect customers against fraud.

The Banking Code already provides much of the protection demanded by this recommendation; specifically protecting customers against losses through card, online banking and cheque fraud.

Sections 12.5–12.9 of the new Code set out clearly what is expected of customers to assist in protecting their payment cards, PINs, chequebooks and online banking account. The level of protection from liability offered to customers is set out in Sections 12.11–12.13. Section 12.13 is the new provision on online banking fraud that states:

> *"Unless you have acted fraudulently or without reasonable care (for example by not following the advice in Section 12.9), you will not be liable for losses caused by someone else which take place through your online banking service".*

The Committee may be further interested to hear of the latest statistics, compiled by APACS from member data, that show that online banking fraud decreased by around 33 per cent in 2007 from £33.5 million to £22.6 million despite a doubling in the number of phishing incidents. The fall was mainly due to the success of banks' continuing customer education efforts, and to their developing capabilities in spotting possible account compromises and preventing fraudulent transactions.

11. *"We further believe that a data security breach notification law would be among the most important advances that the UK 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".*

We are broadly supportive of the Government's response. We would add that the experience of jurisdictions with mandatory disclosure laws is that these laws have rarely achieved what was intended. In many cases disclosures have been made in relation to cases where the potential harm to data subjects was minimal, but the nature of the disclosure mechanism is such that it does not allow data subjects to judge the actual level of risk. It will be important to ensure that risk thresholds for any disclosure scheme are carefully chosen and weighted to ensure that they relate to actual levels of potential harm and we therefore welcome the suggestions made by the Committee in recommendation 12, in ensuring that any disclosure should be appropriate to the level of risk and fit for purpose.

12. *"We recommend that the data security breach notification law should incorporate the following elements: . . ."*

Please see our response to recommendation 11.

13. *"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".*

One of the clear challenges that the financial sector faces is clearly communicating the increasing responsibilities placed on businesses to treat their customer data securely and we would support a co-ordinated approach to this across Government and other agencies.

14. *"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 sponsors".*

The Government makes a number of sound points in its response to this recommendation, but we believe that there is substantial scope for more positive action. Many APACS members are founding supporters of Get Safe Online, and APACS itself has also actively supported and encouraged the initiative since its inception. We welcome the Committee's recommendation that the Government should play a more active role in its promotion. We would encourage the Committee to seek specific commitments from the Government for further increasing the profile of Get Safe Online, and to explore other proactive measures.

The Get Safe Online site is an example of "pull" education, in that it largely relies on people to seek it out, but experience shows that a strategy of "push" methods can be far more effective when communicating complex and unfamiliar concepts. The Government should be encouraged to either lead or fund an aggressive and high profile public information campaign to highlight the risks of e-crime and the measures that consumers and businesses can take to protect themselves.

15. *"We recommend that Ofcom not only sponsor the Get Safe Online project, but that it take responsibility for securing support from the communication industry for the initiative".*

We have nothing further to add to the Government's response.

16. *"We further recommend that, in addition, the new kite mark for content control software, Ofcom work with industry partners and the BSI 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 the kite marks, might be appropriate".*

We are broadly supportive of the Government's response.

17. *"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 safety".*

We believe that the Government could and should be doing much more to promote personal internet security. Although adults are an important part of the mix, we believe that it is of vital importance to promote sound security behaviours and attitudes in the young. A more comprehensive programme of computer security education in schools and colleges, incorporated into the National Curriculum and/or associated ICT courses, as opposed to one-off campaigns, would be an enormous step forward in ensuring that the next generation enters the online world in safety. The Internet has rapidly become a vital part of most peoples' lives and is right that the educational system allocates the appropriate level of resources to ensure that people use it safely.

18. *"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".*

The Government's response on the use of the Computer Misuse Act 1990 and the Police Act 2006 are correct in principle. We would support the Committee in encouraging the Government to ensure that law enforcement and national security functions are appropriately skilled and tasked. We also feel that the phrase "*regardless of the use to which it is put*" goes too far as it could include many perfectly legitimate distributed computing applications that otherwise exhibit many "botnet-like" behaviours and we would encourage the Committee to define its area of interest in terms of harm. For example where bots are run without the knowledge of the owners of the computers involved, for purposes which are criminal.

19. *"We recommend that the Government, in partnership with ACPO and SOCA, develop a unified web-based reporting system for e-crime".*

Although we accept the Government's response that the National Fraud Reporting Centre (NFRC) could provide some of the benefits of the Committee's recommendation, not all online crime manifests itself as fraud, so we would encourage the Committee to continue to support the creation of a unified e-crime reporting system operated by specialised law enforcement agencies. Having said that we do see a potential role for the NFRC in acting as a portal for the reporting of crime, which is then channelled to specialist units.

20. *"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 support the Government's response to this recommendation.

It is important to note that the change in law relates to the recording of crime—where industry figures were always in excess of police figures—and does not relate to the responsibility of law enforcement to investigate any fraud-related crimes.

21. *"We therefore recommend the establishment of a network of computer forensic laboratories, under the aegis of the proposed Association of Chief Police Officers (ACPO) national e-crime unit, but with significant central funding. We further urge the Home Office, without delay, to provide the necessary funds to kick-start the establishment of the PECU, without waiting for the private sector to come forward with funding".*

We strongly believe that a dedicated and specialised law enforcement body with a national remit will be the most effective approach to combating e-crime, and represents a critical capability that is currently missing in the UK. We encourage the Committee to press the case strongly for substantial Government support for Public Employees Credit Union (PECU) in order to ensure that it is appropriately funded and resourced with the skilled staff required.

22. *"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 UK fulfils the spirit as well as the letter of Article 25 of the Convention, we recommend that the Government review procedures for offering mutual legal assistance in response to requests for help from other countries in investigating or prosecuting e-crime".*

We do not feel that the current arrangements for mutual legal assistance are sufficient to deal with the phenomenon of e-crime. The experience of the banking industry at least has been that these arrangements raise considerable issues regarding speed and effectiveness of response. Additionally the scope of current arrangements are not well suited to the demands of dealing with the high-speed borderless nature of e-crime.

23. *"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 Id 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 of internet-related crime.*
- *We believe that the sentences 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."*

We support the Government's response to this recommendation, particularly on the matters of principle raised.

Memorandum by Nicholas Bohm

Introduction

1. I am a member of the Law Society's Electronic Law Committee; these comments are made in my personal capacity.

Recommendation 1—collection and classification of data about e-crime

2. The Government dismisses this recommendation on the ground that crimes are recorded according to the offence prosecuted, and not the tools used to commit them. This misses the point. What e-crimes have in common is that they require particular skills to investigate them, and that they lack an ordinary location because, they are often committed in large batches affecting victims in many different places at much the same time. The development by law enforcement bodies of the necessary skills, and the effectiveness of their work, and the priority it is given, are all liable to be affected adversely by the lack of clear information about the incidence of e-crime that results from its dispersal amongst information about other crimes which are legally similar. I find the Government's attitude regrettable.

Recommendation 2—the risk of criminalising the work of security researchers

3. The Government rejects the Committee's view that security researchers are at risk of being criminalised because of the recent amendment to the Computer Misuse Act. The provision at issue is one under which:

> A person is guilty of an offence if he supplies or offers to supply any article believing that it is likely to be used to commit, or to assist in the commission of, an offence under [other provisions of the Act].

For this purpose "article" includes software. The problem is that most software security tools, and especially software itself, are inherently likely to be misused by someone sooner or later because if they are useful for testing security, they are useful for breaking it. The provision would be less alarming if it laid down that a supply or an offer was an offence only if the supplier or offeror believed that the thing supplied or offered was likely to be used *by an identifiable recipient or offeree* to commit an offence. It does not say that, and it is not clear that it has that meaning. The Government is therefore wrong to deny the existence of the risk created by the amendment.

4. The Government nevertheless acknowledges that legitimate security researchers should have confidence that the new offence will be used appropriately, and its response in October 2007 implied that guidance to be issued by the Crown Prosecution Service would provide the basis for that confidence. That guidance has since been issued, and signally fails to fulfill the expectations thus aroused. While it helpfully advises prosecutors

that security tools have both lawful and unlawful uses, it lays down tests a prosecutor is advised to apply (in order to decide whether someone who supplies them can be shown to have believed they were likely to be used for misuse). These tests amplify the anxieties of security researchers rather than calm them. Prosecutors are advised to ask themselves the following questions:

— Has the article been developed primarily, deliberately, and for the sole purpose of committing a CMA offence (ie unauthorised access to computer material)?

— Is the article available on a wide scale commercial basis and sold through legitimate channels?

— Is the article widely used for legitimate purposes?

— Does it have a substantial installation base?

— What was the context in which the article was used to commit the offence compared with its original intended purpose?

5. The first of these questions will not of course trouble a legitimate researcher (and if it is answered in the affirmative, the remaining questions are irrelevant). The purpose of the second, third and fourth questions is presumably to help a prosecutor distinguish the usual behaviour of legitimate suppliers of security research tools from the behaviour of others. The questions are therefore clearly based on the author's assumptions of fact, about the usual operation of the world of security research. It is more than a little unfortunate that those assumptions are profoundly ignorant of reality.

6. The last 15 years have been marked by the rapidity with which new software is introduced and developed. Attacks on the security of computers and networks have been introduced and have evolved with equal rapidity, and so have defensive and testing tools. Of necessity, the world of computer security research is one in which security tools are developed rapidly by relatively informal collaborative networks of researchers, discussed at conferences or on Internet mailing lists, and published in the ordinary course of academic publishing as well as made available on websites which anyone can access. There are large numbers of such tools, evolving all the time, and available from large numbers of websites visited by large numbers of people. An example is http://nmap.org/, a site which appears to be outside the jurisdiction of the United Kingdom, and claims 40,000 subscribers to its mailing list. In the face of this reality, none of the second, third and fourth of the CPS questions serves the slightest use in distinguishing the legitimate provider of security tools from anyone else. (The final question cannot be answered at the time of supply or offer, since the offence will not yet have been committed, so that it can provide no comfort to a legitimate supplier to know that it will be asked, whatever its use may be to a prosecutor.) The CPS seems to think that security research tools are handled like dangerous pathogens or radioactive isotopes; or perhaps in truth it feels that they ought to be, and that the amended legislation can bring this about. Perhaps an analogy may be considered. Motor vehicles are dangerous things. About 30,000 people are killed or seriously injured in UK road accidents every year. But if it were made an offence to supply a motor vehicle, believing that it was likely to be used to commit a road traffic offence, then there would be a rapid end either to the motor trade or to the government that introduced the legislation.

7. The Government's reply regrettably fails to acknowledge the real risk created by the amendment, and the CPS guidance is a disaster. If security researchers are made to feel that they are at risk of prosecution unless they treat security tools like the smallpox virus, we shall all be the more insecure as a result.

Recommendation 6—removal of "mere conduit" immunity where ISP has been notified that it is serving a compromised machine which is sending out spam or infected code

8. The Government points out, quite rightly, that such a change cannot properly be made without a change to the Ecommerce Directive. It does not favour such a change, observing, ". . . we believe that the [ISP] industry can do more to identify and aspire to best practice in this area. We believe that this holds out more prospects for innovative solutions than impractical solutions about changing liability models". While I agree that in this case it is not appropriate to change the liability model, I take the view that what is needed is a regime of penalties for ISPs who fail to isolate compromised machines.

9. It is very unusual to make one person liable for the wrongs of another, even when that person is in a position to put an end to continuing wrongs by the other and refrains after notice from doing so. (The vicarious liability of an employer for the acts and neglects of an employee acting in the course of his employment, stands out as a special case. The employer takes the benefit of the employee's work, and must stand the risk; and it is for the benefit of third parties to give the employer an incentive both to manage employees properly and to maintain insurance.) In general, inaction cannot logically be the basis for liability unless there is a duty to act. Duties to act for the benefit of another are normally imposed by the law only where there are close ties between the parties. A parent's duty to nourish a child is an example. In the case in question, the relevant relationship is

that between an ISP and the persons liable to suffer economic loss by reason of the ISP's failure to close an account from which spam or infected code are being distributed. This is very far indeed from being the sort of close relationship which would give rise to a duty to act, so that removal of the "mere conduit" exemption would by itself have no effect without a positive change in the law. That is not to say that the case for such a change could not be made, but I do not think it has been made convincingly. This is not a context in which imposing liability on an ISP for inaction would provide a satisfactory incentive. The damage which the ISP's action would be designed to avert, would fall on huge numbers of people in numerous jurisdictions. In most cases the damage would be small in amount, often less than the cost of quantifying it, tracing the person liable, giving notice, waiting for more loss to accrue, tracing that to the same source and then applying for compensation. The UK legal system does not encourage class actions, and the risk of the loser having to pay the winner's costs is discouraging. The pressure applied to ISPs would be capricious and slow.

10. In the result I agree with the Government's conclusion, though for a reason very different from the one it gives. The Government's reasoning is indeed a matter for considerable concern, if it implies that in principle exhortation is preferable to the incentive effects of suitable liability models. Perverse incentives arise wherever the creators of security risks do not suffer the consequences that flow from them. Changing the applicable liability model where appropriate, so as to make the polluter pay, is an important part of the strategy necessary to improve the security of the Internet. While agreeing with the Government's conclusion, I would reject its reasoning.

11. The Government and the Committee are at one in thinking that the worst ISPs need to behave more like the best in their treatment of rogue machines on their networks. This seems to me a case where the application of a regime of regulatory penalties might be appropriate. The Financial Services Authority has been notably willing to impose substantial penalties on financial institutions for security failures, and if experience does not show these to be dissuasive, there is no reason to doubt the willingness of the FSA to increase them until they are. There seems to be no policy objection to the imposition of such a regime; the Government has announced its willingness to compel ISPs to disconnect the amateur copyright-infringers whose activities so aggrieve the music industry; the isolation by ISPs of machines sending out spam and infected code seems at least as deserving an object of compulsion, and as an endeavour it has the advantage of being both technically feasible and supported by most ISPs, provided that it is aimed precisely at the target I have described, and is not subverted into a scheme for the general regulation of ISPs.

Recommendation 8—exploring the introduction of vendor liability at European level

12. I found the Committee's arguments in support of its recommendation convincing. (My own caution when giving evidence to the Committee on this question was due principally to the dangers of producing unintended consequences by legislative intervention in a complex multi-jurisdictional field.) The Government accepts no more than that there is scope for further discussion at the European level, and claims that this is already taking place as part of the ongoing Review of the Consumer Acquis. As one of the expert stakeholders accredited to the European Commission in connection with the review of the consumer acquis (and the related endeavour to prepare a "common frame of reference"), I have observed and participated in discussions on legal issues in this field. I have not noticed any discussion about any change to the liability model applying to vendors in the present context; nor has the topic arisen at any of the helpful meetings between the UK stakeholders and the Ministry of Justice to deal with the progress of the review. No change will occur without active efforts by the Government to promote it, and the Committee is right to press the Government to make those efforts.

Recommendation 9—the need for Government to ensure businesses have adequate incentives to protect customers' personal data

13. The Committee's concerns have turned out to be well-founded; and the Government's denials that losses of personal data were increasing, or that it was indifferent to them have been cast into the awkward light of reality by the deluge of reported data losses that began to emerge in such quantity not long after its reply was published. One might hope that the Government would reconsider its response.

Recommendation 10—making banks effectively liable for losses by electronic fraud

14. The Government's reply is that no change is necessary, because the Banking Code ensures that the banks reimburse fraudulent losses unless the customer colluded in the fraud or caused it by negligence. This merely repeats the position taken by the banks, and evades the essential point without addressing it at all. That point is that the banks' "proof" that the customer colluded in the fraud or caused it by negligence is a proof by assertion not based on evidence openly produced for testing. In practice the banks assert that their systems

have operated without error and show that the customer's card was used with his PIN, and from that they infer that the customer "must have" colluded in the fraud or caused it by negligence, because they say there is no other plausible explanation. They decline to produce the internal system evidence on which they claim to rely, on the ground that it must be withheld to protect the security of other customers. The Financial Ombudsman Service accepts all this without challenge. The few customers who have brought claims in the courts have not had adequate legal and technical support. The courts (normally the County Court) have been unduly impressed by the banks' claims about the need for secrecy, and have had significant difficulty with highly technical evidence. In effect, the banks have deployed systems which have enabled them to decide which customers are innocent victims of fraud and which of them "must have" colluded in the fraud or caused it by negligence. The issues are discussed in some detail at www.fipr.org/080116huntreview.pdf, a submission to Lord Hunt's review of the Financial Ombudsman Service made by Professor Ross Anderson (another witness to the Committee) and me.

15. The banks protest that if they cannot rely on their present way of "proving" that a customer must bear a disputed loss, they would have to pay the claims of careless or fraudulent customers. But they are the authors of the systems which have led to this dilemma, and have derived huge financial benefit from using them. If they were forced to meet claims that they could not disprove by open evidence, they could decide whether to stand the losses or to improve security, whichever they preferred. Among the simple improvements would be the deployment of cameras to photograph users of cash machines, and among the more complex would be the development of genuinely trustworthy authentication devices on the basis of the European Committee for Standardization's FINREAD standards published some years ago.

16. The Government's evasive dismissal of the recommendation is regrettable. It is to be hoped that when the Treasury undertakes a consultation on the implementation of the Payment Services Directive there may be an opportunity to address these issues again.

Recommendation 11—a data security breach notification law

17. The Government's reply, to the effect that laws of this kind were of doubtful value and only brought into force in the United States because of its lack of a European approach to data protection, can now be seen to be smug and overconfident. Indeed, the Government has been forced by events to undertake extensive data breach notification on its own account. I can do no more than express the hope that the same events will bring about a change in the Government's view of the recommendation.

Recommendation 20—need to review reporting of fraud to banks rather than the police

18. The Government continues to argue for the desirability of arrangements under which customers report a fraud to their bank, and the police will only treat it as a crime if the bank reimburses the customer and itself reports the fraud to the police. The Government claims that where customers are not refunded they retain the ability to report these matters directly to the police, where crimes should be recorded. I am sceptical of this latter claim, and suspect that where the bank refuses to report a fraud, the police may well refuse to accept the customer's claim that there was one. There ought to be an early check that the system really works as described.

19. A system which depends on a decision by a bank on whether or not a customer has been defrauded is flawed by the fact that the bank has a direct financial interest in denying the customer's claim. Moreover, there is not the slightest need for reliance on such a decision. If a customer's account has been charged with a transaction for which the customer denies responsibility, there are only three material possibilities:

- the transaction was carried out by a third party in circumstances where the customer is not responsible—the bank has been defrauded by the third party;
- the transaction was carried out by a third party relying on carelessness by the customer such that the customer and not the bank is responsible—the customer has been defrauded by the third party (the carelessness does not excuse the fraud); or
- the transaction was carried out by the customer or by someone in collusion with him—the customer has attempted to defraud the bank.

(I leave out of account cases of mistakes by the customer or the bank which are resolved between them.) It follows that all such cases should be reported to the police, whether or not the bank reimburses the customer.

Generally

20. Events since the publication of the Government's reply to the Committee's Report, have revealed to the public the existence of serious flaws in the Government's understanding and implementation of data security. Its reply demonstrates that those flaws are characteristic of a much deeper failure by many ministers and officials to adapt to the impact of technological change, or indeed to grasp its implications adequately or at all. Whitehall has become a cloister, sheltering its inhabitants from contact with many painful realities. As a result, much of its response to the Committee's blast of fresh air has been lamentably defensive. I hope that the Committee will not let its sword sleep in its hand.

9 March 2008

Memorandum by the Child Exploitation and Online Protection Centre

Introduction

Further to its publication on Personal Internet Security in August 2007, The House of Lords Select Committee (Science and Technology), has invited comments on the Government's response to that report (published by the Home Office in October 2007). In doing so, this reply will consider the primary issues pertaining to the online risks posed to children and adults.

Comment on the Increased Use of the Internet

The expansion in the use of the Internet has brought about many positives to young people and their parents, both from an educational and business perspective as well as social interaction through Social Networking sites, instant messaging, gaming and with the increase in the internet and mobile phone convergence, young people are presented with an ever increasing diverse opportunity to learn, explore, to meet new people and have fun. This capacity for interaction between young people throughout the world will continue to increase as technology progresses. There is a digital knowledge gap between parents and children and this could go some way to explain some of the concerns over safety on the internet.

In general terms, the Government felt that the report implied that there was a "loss of public confidence in the use of the internet" and that "lawlessness was rife." Whilst the report from the House of Lords did not explicitly state this, the report is in danger of drawing conclusions about the extent of crime that is committed on the internet and the level of anxiety from members of the public that are not supported by facts and figures. Whilst the report acknowledges the lack of research and data collection of risks and the types of crimes committed, conclusions must not be drawn without supporting evidence.

The internet is a fabulous tool, the use of which will only continue to expand and I welcome the Government's acknowledgement of the importance of ensuring personal security against the risks posed to users on the internet. I am in agreement with the Government in that it is not only the responsibility of the individual to take steps to ensure their safety. There must be a multi-faceted approach between government, educators, law enforcement, industry and child protection experts to ensure the personal security of any user of the internet; it is not the sole responsibility of any one of those groups. Education is one of the key factors to empowering children and adults to learn about potential dangers and to know what to do if they have concerns. Whilst the Get Safe Online initiative includes advice on fraud and the protection of personal details, CEOP's "thinkuknow" education campaign, has developed a series of specific programmes for five to seven year olds, eight to eleven year olds and twelve to seventeen year olds. There is also specific advice for parents. The provision of advice in a way that engages not only children but their parents is vital.

I also support the Government's view that the use of the internet as a tool for committing crime must be taken seriously, and that it is important for users to have confidence in their security on the internet. I appreciate that the Government does not want to "impose additional burdens on business", but feel it is important that those who are in the business of providing internet services and hosting services must continue to work more closely together as part of this multi-faceted approach, with Government and law enforcement to identify steps to increase safety online. To an extent this is already happening and there are some excellent examples of this approach in the partnership work undertaken at CEOP. Industry should put children's welfare at the heart of their products and services whilst making future developments in technology possible.

Within the current framework of self-regulation, CEOP is/should be working in partnership with industry to provide knowledge and insight of how their services are being misused and as an instrument of crime. When this is combined with industry's technical skills and user engagement expertise they can take this insight drawn from law enforcement into practical business-driven solutions aimed at minimising the risks and harm to children and developing confidence in their brands from parents, carers, educators and the children themselves.

CEOP endorses the majority of comments made by the Government in responding to the report on Personal Internet Security and the emphasis that is placed on the close working collaboration of interested parties, including industry, government, law enforcement and academia. Further to this, it wishes the Committee to note the following points:

— We endorse the view that there need to be improvements in how data is collected in relation to e-crime. However, we feel that experts involved in such data collection must include law enforcement and prosecuting bodies. We agree with the Government that data collection should be in reference to the type of offences that can be committed but should include information into how the internet is used as a tool to commit crime. The remit of this proposed group would also need clarification as to what the purpose of such data collection would be.

— We support the Government's view that there is a need for interested parties to have clear focus for the need for personal safety. Whilst the report's recommendation (no.4) states that there is a need for the Government to develop a more holistic understanding of the responsibility for personal security, we believe this is one recommendation that should be directed to all interested stakeholders. All parties need to be more open minded to make personal safety a priority.

15 April 2008

Memorandum by the Children's Charities' Coalition on Internet Safety (CHIS)

In relation to levels of public confidence in the internet (page1, Introduction), there is no doubt at all that, at least as far as children's and young people's use of it are concerned, there is a continuing, high level of anxiety and lack of trust, a fact which is constantly being evidenced in research. It is also a fact which was implicitly, if not explicitly, recognised by the Prime Minister when he commissioned Dr Tanya Byron to report on these very matters. Her report is expected on or by the 31st of this month. I might add that, right now, there is more big and small "p" political activity taking place around aspects of internet policy than has ever been the case hitherto within the United Kingdom. This hardly betokens a sense that public policy is settled or that there is a widespread consensus about it.

The fact that there is continued, strong growth in internet usage and in trading on the internet does not necessarily disprove the notion that there is a high level of public disquiet about it. It could be more a case of force majeure.

There are some things you can no longer do, in a practical sense, unless you use the internet. If you want the cheaper holidays or the tickets for your favourite band you really must go online, but that does not necessarily mean you entirely trust the online environment or that you feel completely comfortable about using it.

Hardly a month goes by without another report appearing in the press of some company or other, or some public agency or other, losing or misplacing data, or of credit card details being wrongfully exposed online through a security breach on a web server. It does not follow that simply because people nonetheless carry on using the internet to buy and sell things or to submit forms to their local Council or to the Government, that they do not care about these things or they believe they are merely isolated incidents which are being satisfactorily dealt with. More likely, it probably just means they feel they have no real choice but to carry on and bear the risk.

Moving on, again on page 1, the Government refers to the question of the regulatory burden. I am sure everyone agrees that "imposing additional burdens on business" is not an end in itself, much less is it a desirable end in itself, but it cannot be the starting point of policy discussions. The object, surely, must be to take a view about what the policy objective is or ought to be and then to devise the best possible means of delivering it, whilst accepting there should never be any gratuitous or unnecessary administrative or other burdens placed on anyone, be they a business or any other kind of enterprise.

On page 2, paragraph 1, the Government appears to rule out the possibility of changing the way information is collected on how crimes are committed to reflect whether or not computers or the internet played a major part in their commission. This is highly regrettable and it is hoped this point can be reconsidered.

We agree that the decision about whether or not to prosecute someone, in general, ought not to be affected by any consideration of the tools used to commit the offence. However, in relation to improving our ability to devise improved crime fighting strategies eg to protect children online, it must be in everyone's interests to be able to see how the new technologies are shaping criminal behaviour. At the moment, absent that data being collected on a systematic basis, everyone has to rely on one off studies or else we are thrown back on anecdotal evidence. That cannot be right.

On page 5, the Government refers to the issue of "mere conduit" status. Clearly the Government is right to say it cannot act selectively on European legislation, but would they support, or themselves bring forward a proposal to change the current provisions on mere conduit status? We hope so, both for the reasons given by the Select Committee but also because we know, because ISPs and other online providers have told us this repeatedly, the current Directive introduces a positive incentive to do nothing. It is true that some ISPs and other online providers choose to act, despite the legal risk they thereby take on, but it is also undeniably true that others choose not to act precisely in order to avoid attracting any potential or additional liability. In other words the Directive threatens to punish the responsible company that wants to engage proactively to do the right thing, and it rewards the provider who is happy just to sit back and wait to be told there is a problem. Again, that cannot be right.

17 March 2008

Memorandum by eBay and PayPal

1. *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 the recording of all forms of e-crime.*

We support this recommendation and welcome the Government's commitment to set up "a small, high-level Government/industry working group to develop a more co-ordinated approach to tackling crime committed using computers as the medium". We would be delighted to be involved in such a working group.

On the other hand we disagree with the Government's conclusion that there is no need to "devise a classification scheme for the recording of all forms of e-crimes". While we understand the Government's view that prosecution should be based on the offence rather than the tools used to commit that offence, it would be helpful to record, for example, the number of frauds perpetrated by means of spoof emails.

We believe that the establishment of a framework to collect and classify data on e-crime would be beneficial in defining the scale of the problem, and could provide a helpful tool for companies actively fighting e-crime. Such a framework would also be helpful in shedding light on the real scale of the problem, and the threat it poses to the development of the Internet economy. Furthermore, common data and definitions will help the work of law enforcement and the judiciary.

The Network

4. *It is time for Government to develop a more holistic understanding of the distributed responsibility for personal internet security.*

We agree that responsibility for personal Internet security needs to be shared among industry, law enforcement, government and users.

While we appreciate the efforts led by the Cabinet Office and all other departments involved, we would welcome a coordinated strategy involving all Government departments, agencies and law enforcement.

6. *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.*

We agree with the Government's position on preserving the "mere conduit" principle for ISPs.

However, we believe that Internet connectivity providers (generically referred to in the report as ISPs) can, and should, do more to detect bad traffic in a timely fashion, whilst being granted a safe harbour from legal liability, for the time necessary. Furthermore, web hosting providers—particularly those based overseas—could do more to reduce substantially the time taken to respond to spoof site shutdown requests—for example,

by providing 24/7 support to deal with reports from recognized intellectual property owners or experts. This would make a huge difference in our ability to combat phishing and could substantially reduce the impact of fraudsters and e-criminals on consumers and companies alike.

Using the Internet: Businesses

9. *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 a position to prescribe the security precautions that should be taken; however, they do have responsibility to ensure that the right incentives are in place to persuade businesses to take the necessary steps to act proportionately to protect data.*

We agree that security precautions should not be prescribed by legislation. We believe that a more useful approach would be to focus on defining a common set of standards which data custodians should follow. These standards should be set by relevant industry standard bodies, rather than through primary legislation, to ensure that the standards are updated in a timely fashion as technology and best practice evolve. The Data Security Standards developed by the Payment Card Industry Security Standards Council, which are now being rolled out globally, represent a best practice in this area and could be an example to other sectors.

11. *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 or urgency.*

We agree with the Government that a data security breach notification law would not necessarily be the best solution. Our experience in the US has shown that these laws are not a cure-all remedy. On the one hand, these laws have been useful in bringing the risks of identity theft to the public attention and in shining a light on those organizations which fail to securely manage their customer data. On the other hand, the standard for which notification is required is often too low which has led users to disregard such warnings. To the extent that legislation is necessary, it should focus on notifying users when there is a reasonable likelihood of actual harm or identity theft that could result in financial loss—for example, it should take into account whether data is personally identifiable; and if so, whether it is encrypted or not.

14. *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 sponsors.*

We look forward to the outcome of the CSIA's "Work with Direct Gov and Business Links in rationalising the approach to providing internet safety information to customers." We believe the Government could do more to make available to "Get Safe Online" its multiple channels of communication to deliver messages of security awareness to internet consumers and small enterprises, and sponsorship opportunities to larger enterprises.

The "Get Safe Online" message needs to be an integral part of all Internet security conversations at the highest levels of Government and not be limited to an annual speaking commitment.

We therefore welcome the Committee's support of the "Get Safe Online" initiative and their calls for enhanced support from the Government and Ofcom. As a founding partner of Get Safe Online, eBay has played a key role in getting this initiative off the ground. However, we do not believe it is sustainable in the long run to expect a relatively small number of private sponsors to meet such a large share of the ongoing costs of this programme. We therefore fully support the Committee's recommendations to recruit new sponsors who are capable of funding the next phase of the "Get Safe Online" campaign or providing support in kind.

Policing the Internet

19. *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 ecrime.*

We strongly support the creation of a unified, web-based reporting system for e-crime. We believe this would be beneficial to industry and users while facilitating the work of law enforcement.

We therefore welcome the Government's commitment to consider this recommendation. We would argue that while there is an overlap between the Fraud Review National Fraud Reporting Centre (NFRC) proposal and the proposed ACPO national e-crime unit to tackle e-crimes, the two will serve different purposes. We look forward to concrete and immediate action from the Government to establish a national e-crime unit.

However, any reporting system should not serve as a black box into which consumer complaints are effectively "dumped", with no clear follow up. Of equal importance to reporting mechanisms is an effective "triage" system which can direct consumers to the most appropriate source of help, whether that is industry, government or law enforcement.

21. *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. We further urge the Home Office, without delay, to provide the necessary funds to kick-start the establishment of the Police Central E-Crime Unit, without waiting for the private sector to come forward with funding.*

We strongly second calls for increased resource allocation to law enforcement. We actively co-operate with law enforcement on a regular basis, assisting them in their investigations and training them on how to work with eBay and PayPal. Despite our many successes, we are confident that even more could be achieved with the right resources and training. We therefore look forward to the establishment of an appropriately resourced national e-crime unit. We would also welcome the development of a SPOC process for e-crime within the Police.

Memorandum by the Metropolitan Police Service (MPS)

Introduction

The Government does not agree with the implication that "*the public has lost confidence in using the internet*".[2] *The Government supports this position quoting substantial year-on-year growth in usage of the internet. We welcome and acknowledge this growth but would comment that both anecdotal evidence and survey evidence indicates growing concern over internet security. Interactive Retail in Media Group (IMRG) estimate that on-line trade is suppressed by 20 per cent through fears over internet security. The Demos survey conducted on behalf of the Post Office in December 2007, reveals that fear of fraud is the single biggest factor deterring the over 50 age group from engaging on-line.*

The following quote is from a letter to the Editor of the *Metro* Newspaper published on 14 March 2008 and is indicative of widespread public opinion. "*It is not surprising that credit card fraud is booming when it is hardly ever investigated. When someone hacked into my online account the company treated it like a civil dispute and told me I'd have to serve a writ on them to obtain the identity of the thief. More recently, another online account of mine was hacked and money transferred to a gaming account . . . . . Shoplifters who steal trivial sums are processed by the courts on a daily basis, while, it seems, people who steals thousands of pounds in online fraud are not even pursued*".

Since the publication of the Report and the Government response to it, the personal data of more than half the population of the United Kingdom has been compromised by government departments. As industry conducts a review of its own data handling and storage processes, more disclosures of compromised data have been made. It is reasonable to assume that many more identity compromises have not been disclosed. In less than six months public trust in the ability of government, and to a lesser extent the private sector, to protect the identity of the individual has been completely undermined. When coupled with the existing fears of internet use by large sections of society, it is no longer reasonable to assert that the public retains confidence in using the internet.

The Government "*refutes the suggestion that the public has lost confidence in the internet and that lawlessness is rife*".[3] We, too, anticipate increased uptake of the internet by the personal user despite these fears of lawlessness. There exists no empirical evidence of the extent of criminality enabled by the internet, either within the UK or beyond. A recent Distributed Denial of Service (DDOS) investigation undertaken by the MPS, revealed that of 104 UK companies targeted in the attack, only one company reported the matter to police.

The MPS has suggested that allegations of internet-enabled crime be uniformly categorised at the reporting stage, to provide a true and accurate picture of the extent of this "lawlessness". The MPS has begun the process in London and *e-crime Wales* has a similar initiative across the four Welsh police forces. The current Her Majesty's Inspectorate of Constabulary (HMIC) inspection of Forces, includes two questions relating to force response to e-crime. We hope that this will encourage other Forces to consider quantifying internet-enabled criminality and, thereby, provide an accurate overall picture of the problem in the future.

In respect of new legislation the Government "*does not consider that imposing additional burdens on business is the best way forward*".[4] The MPS does not propose additional legislation in this field. However a robust enforcement policy, and the resources to undertake it, must be pursued by the Office of the Information

[2] Page One—paragraph 3.
[3] Page One—paragraph 4.
[4] Page One—paragraph 5.

Commissioner. The MPS is concerned that any Data Breach Notification legislation will result in additional referrals to police for investigation along with the responsibility for the crime prevention action necessary. The Government must consider in full, any impact assessment undertaken prior to such legislation.

The Government has stated in its response that it "*will consider the proposals to create a law enforcement unit to tackle crimes involving computers*".[5] This proposal was formally submitted to the Government by the MPS on behalf of ACPO, in mid-October 2007. The Government raised a series of questions in relation to the Business Case for such a unit, which in turn were responded to in mid-December. At the time of writing we await a formal decision from the Government upon the proposal.

Recommendation One

The Government proposes the creation of a "*small, high level Government/Industry working group to develop a more co-ordinated approach to tackling crime committed using computers as a medium*".[6] To some extent this forum exists in the National E-crime Strategy Group (NeSG) chaired by SOCA and on which the Home Office is represented. To promote the co-ordinated approach espoused, a broader representation is required than suggested. Law-enforcement, academia and civil society must play a part in the formulation of strategy. Such a "working group" must not replicate similar fora already in existence.

The MPS experience is that high-level discussion groups will not deliver on-the-ground short-term solutions to the current problems of policing e-crime. These difficulties include increasing demands, increasing backlogs and decreasing resources.

Recommendation Two

The Government does not accept the view that Section 3A of the Computer Misuse Act 1990 places security researchers in jeopardy.[7] The MPS holds the same view. Before a successful prosecution could be undertaken the CPS would have to take the view that a prosecution was in the public interest and that *mens rea* was made out. This would not succeed in the case of honest research.

Recommendation Four

The government is "*actively pursuing ideas with the Internet Service providers as to how they might work even more closely with their customers to prevent harm . . .*"[8] The MPS holds the view that Internet Service Providers are uniquely positioned to play a key part in protecting society from the more damaging effects of internet abuse. The MPS supports a voluntary code of co-operation rather than a legislative approach. The MPS is keen to see results from these discussions with the ISPs and would welcome the opportunity to participate.

Recommendation Six

It is the experience of the MPS that the more responsible ISPs do actively assist with the closure of websites and email addresses that abuse the Network. It is also true to say that some ISPs exercise the "mere conduit" excuse to avoid any responsibility for content. We do not comment upon the legality of this position, however those that do decline to assist pose a particular problem for law-enforcement. Although Proceeds of Crime legislation and arguably Fraud Act offences may be identified, law enforcement possesses a particular problem in terms of volumes and jurisdiction when enforcing co-operation. The MPS supports a Voluntary Code of conduct for the ISPs before legislation is contemplated.

Recommendation Nine

It is understood that the Government's response to this question was drafted prior to the series of data compromises that have captured headlines in recent months. Few would now agree with the statement that "*we do not agree that the incidence of loss of personal data is on an upward path*".[9] The benefit of these recent catastrophic losses may be to force industry to examine their own protection systems and processes. There is anecdotal evidence that this process has begun. The MPS disagrees with the Government view that the current

[5] Page One—paragraph 6.
[6] Page Two—paragraph 3.
[7] Page Four—paragraph 3.
[8] Page Four—paragraph 3.
[9] Page Six—paragraph 4.

data protection regime is robust enough to encourage business to take this issue seriously. Although the MPS would like to see firm enforcement of current legislation we do not favour the enactment of Data Breach Notification legislation as this would have considerable, and to some degree unknown, implications for police charged with pursuing allegations referred to it, either directly or by the Information Commissioner's Office.

The MPS does not accept that the Government "*cannot prescribe the technologies or processes that should be deployed to protect information*".[10] The CESG CAP scheme already prescribes the use of certain products across government and those wishing to trade with government.

Recommendation Eighteen

The MPS would support this proposal for criminalizing the use of a BotNet, however it would be necessary to show that the computers that formed a BotNet were used without the consent or knowledge of the owner.

Recommendation Nineteen

The MPS does not support this recommendation for the creation a web-based reporting facility for e-crime. We concur that the NFRC will provide, to a large extent, such a facility in respect of allegations of fraud. The proposed Police Central e-crime Unit would, however, provide a web-based "notification" facility for e-crime. The MPS (as ACPO lead-force for e-crime) is engaged with the NFRC to ensure that the respective web-portals, currently under construction, are complimentary. The "notification", as opposed to a reporting facility, allows for the timely collation of actionable intelligence without the administrative burden of duplicating formal crime reporting.

Recommendation Twenty-One

The MPS welcomes the Government's commitment to "*ensure that all efforts to combat crimes online are co-ordinated*".[11] The MPS champions the concept of a co-ordinated police response to e-crime. Without a co-ordinated police effort the Government concept of multi-agency co-ordination is unrealistic. The creation of a centralised police e-crime coordination unit is essential to respond adequately to 21st Century criminality. This new threat is not simply "old crimes committed with new tools" but also comprises hitherto unrecognised risks to society. The House of Lords report recommends the initial funding of such a unit "without delay". These new threats do not fall within traditional "core policing" areas of responsibility and do not fit with our system of geographical policing delivery. We urge the Government to recognise this and to accept this recommendation.

Recommendation Twenty-Two

It is the experience of the MPS that the Mutual Legal Assistance process is too slow to secure "real-time" and "short-lived" data evidence. The introduction of a European Evidence Warrant may assist the process but it is anticipated that the current practise of relying on the Interpol and G8 contact arrangement will continue. As almost all internet investigations require liaison with law enforcement partners abroad, the MPS supports this recommendation for a comprehensive review of the process.

Memorandum by Symantec

About Symantec

Symantec is a world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries.[12]

Symantec welcomed the publication of the House of Lords report into Personal Internet Security in August 2007. Since its publication the report has encouraged discussion around the responsibility of security on the Internet and has helped to highlight and raise greater awareness of the need to fight e-crime in the UK. In preparation for the forthcoming debate on the Committee's findings Symantec appreciates the opportunity to provide additional input to the Committee.

[10] Page Six—paragraph 4.
[11] Page 11—paragraph 4.
[12] www.symantec.com

The aim of the following submission is to provide supplementary evidence in response to the recommendations made by the Committee and the Government's response to the Committee's report on three key issues:

— Vendor liability.
— Data security breach notification law.
— Establishment of a Police Central e-Crime Unit.

Data Security Breach Notification Law

It is suggested that the recent high profile incidents of personal data loss has prompted wide discussion in the UK on the level of security given to personal information shared, processed, stored and transmitted electronically. Incidents where personal sensitive information, such as financial, contact and employment information, and sensitive identity related data has been lost, stolen, accessed or disclosed without authorisation, are leading to questions and increasingly, demands for answers, by citizens as to what happens if their data is involved in such incidents. Gaining and maintaining the trust and buy-in of citizens that their data is secure and protected therefore represents a potential risk to the future development of innovative, higher value added online services and will be a key challenge going forward for organisations and the Government.

Symantec, therefore, welcomed the Committee's recommendation for the introduction of data breach notification law in the UK as a matter of urgency. While the Government's recognition that such a suggestion warrants further discussion and consideration is understood and accepted, the view that the introduction of notification initially within the UK would not "lead to an improvement" or have an impact on the safety and protection of personal information is, we feel, debatable.

The development and introduction of an appropriately drafted data breach notification legal requirement is seen as an important incentive to increase levels of security and also help raise greater awareness, and reassurance, of how personal data is protected online. It is also suggested that a data breach notification law could help to raise citizen's awareness of the risks their data is being open to and therefore enable them to take appropriate action where necessary. By being given information, citizens can become more empowered to make informed decisions and take measures to protect their identities that may be at risk. Such activities may include monitoring financial accounts for discrepancies, not responding to potential phishing emails related to a data breach or simply ensuring personal information is not disclosed unnecessarily. It can be argued that the action of presenting an individual with a data breach notification letter, for example, could mean that individuals become more aware of the situation and by being fully informed are able to take action they see as appropriate to protect their identity or personal information going forward.

Based on the evidence given in its response, regarding the disjointed approach taken across US States to the introduction of data breach laws, the Government's concerns and questions expressed as to the positive impact of the data breach legislation in the US are understood. However, it should be recognised that if introduced, a data breach notification requirement would simply be an addition to the already effective existing Data Protection legal framework in place in the UK and across Europe. The current European Data Protection law effectively protects the lifecycle of personal data from its collection and processing to its storage. However, the current legal framework does not address circumstances where data is lost or stolen. A legal gap therefore exists that needs to be closed particularly in light of the increase in incidents of data being lost or stolen occurring in Europe. Closing this gap would not only complement the current Data Protection legislation but also serve to enhance the security of data throughout its complete lifecycle.

Symantec does agree with the Government that given the potential impact of legislation in this area it is important that the move towards data breach notification is one which is carefully considered. This is vital to ensure that a clearly defined legal framework and appropriate operational procedures are established that is workable and not burdensome on either citizens or industry. For example, there is further discussion needed on how a data breach notification requirement in the UK would work in practice; fundamentally in the event of a breach what immediate action would an organisation have to take. This includes the definition of an incident that would be considered a "breach" of data and the level of seriousness a breach would have to be to trigger a notification obligation; in addition, as identified by the Government's response, whether companies would be required to notify the Information Commissioner's Office (ICO) before alerting customers. This raises the question of whether the decision to notify customers will rest with the ICO or with the organisation itself. These definitions are a vital part of any data breach legal framework and must be clearly defined so that companies clearly understand when a data breach notification requirement would be triggered. Also any legal requirement that is drafted should include a safe harbour provision to ensure that in the event of a data breach, organisations that can demonstrate an adequate level of data security are relieved from liability and possible legal or financial penalties for the breach.

Nevertheless Symantec welcomed the Government's recognition that any data breach notification requirement should not apply solely to communication provider "in isolation". Recent incidents of data loss in other key sectors, such as finance and retail, indicates a strong argument that companies in all sectors, public and private, that are processing and storing individuals personal data electronically should be required to comply with a data breach notification law. In the latest Symantec Internet Security Threat Report, published in September 2007, education was the highest sector for data breaches that could lead to identity theft with 30 per cent. This was followed by government (26 per cent), healthcare (15 per cent) and the finance sector (14 per cent). The Government's review that if a data breach law is introduced in the UK it should not impact solely any one sector is therefore supported by Symantec.

Given that the European Commission's proposals to introduce a data breach notification law for the communication sector may not come into force until at least late 2009 early 2010, it is suggested that further consideration and discussion is needed on the need for the UK to become a pioneer and lead the way in Europe but introducing an appropriate, and reasonable, data breach notification requirement in the UK and not wait possibly for five years for the European legislative process to introduce breach notification that will only impact one sector. Symantec believe that an appropriate data breach notification law could be effective if applied to all sectors that are processing and storing individual's personal data. However, the steps currently being taken by the European Commission to introduce an appropriate data breach notification requirement across Europe is seen as a step in the right direction.

Establishment of a Police Central e-Crime Unit

The Committee's acknowledgment that the Internet has become a powerful and critical tool in the UK's national infrastructure is reflective of the in-depth investigation and consideration the Committee has given to this important topic. Symantec agrees with the Committee that industry, end users and the Government all need to be doing more to ensure the protection of this resource. In particular Symantec endorses the Committee's recommendation supporting the creation of a Police central e-Crime Unit. The Government's response that consideration was being given to the business case for creation of a dedicated law enforcement unit for e-crime along the lines proposed by the Committee is also encouraging. However, while it is understood that the National Fraud Reporting Centre has been given additional funding in the recent Comprehensive Spending Review to develop a strong "anti-fraud culture", in addition to further investment for policing and a more strategic approach to be taken towards "cutting crime", e-crime was noticeable by its absence in the Government's spending plans published back in October 2007. As we now move into March 2008 it is still not clear whether the business case for the creation of a Police central e-Crime unit will be supported both operationally and more importantly financially.

In its response, the Government acknowledged that national co-ordination for policing in this area could bring benefits to the fight against e-crime in the UK. This view is supported as is the comment that for the creation of any new unit there must be a clearly defined need in order to ensure an effective response. It is agreed that an e-Crime policing unit would need to have clearly defined aims, objectives and goals. However, Symantec believe there is a clear need for a national police presence in the fight against e-crime in the UK.

The recent shift in the online threat environment towards computer related attacks being motivated, not by notoriety, but by economic gain has resulted in individual users, as well as companies, becoming front line targets for cyber criminals. Individuals are increasingly targeted by attacks designed to steal confidential information that can be used to commit fraud and theft. It is understood that such crimes must be investigated and prosecuted as traditional crimes (such as fraud) merely conducted using a new tool (technology). However, it must be recognised that policing resources, focus and training are needed to effectively investigate and address these modern technological enabled crimes. This is why there is a clear need for the creation of a central e-crime police unit that can support law enforcement efforts. The UK is currently one of the most effective and best placed countries in addressing cyber crime. In order for this reputation to continue however, Symantec believe more training and more resources are needed by UK police not just in London but across the whole of the UK. The introduction of a dedicated national e-Crime policing unit would be a step in the right direction to enhancing the UK police's ability to respond to e-crime effectively; at a time when concerns regarding online security risks, arising from spam, phishing, social networking sites and online data theft, may be preventing citizens gaining the full benefits from the Internet. For example results of a recent Get Safe Online campaign survey, to which Symantec is a leading sponsor, indicates that almost one in three UK internet users[13] will not conduct banking online due to their fears about safety and security.

[13] Get Safe Online Survey Published November 2008 www.getsafeonline.org.

Vendor Liability

When the Committee's findings were published in August 2007, Symantec welcomed the Committee's recognition of the importance of ensuring interoperability, consumer choice and a competitive landscape in the information security market. However, the view that software companies should be liable for ineffective products and services offered to users is nevertheless challenged. There is also concern at the Government's response to the Committee which suggested that there is "scope" for further discussion of this issue at the European level. Symantec believe extending the product liability regime of the European Consumer Sales Directive, as discussed in the European Commission's Green Paper, to digital content including software could result in reducing consumer choice and risks the opposite effect of reducing users' security and privacy.

The Committee's suggestion in this area does not take into account the complexity of the IT industry. Essentially software companies cannot be liable for what they do not effectively control. For example, how the customer installs, configures, uses and updates its software. Effective security is a combination of a layered security approach, processes, people and technology. An approach whereby the liability burden is placed on software providers therefore runs the risk of simply putting the burden only on technology and ignores all the other components. Also, it is doubtful that companies would be prepared to take liability for their products unless they can assume a level of control on how the interoperability takes place and ensure it does not affect their applications This may lead to technology providers using more privacy-invasive technologies to control not only the interoperability allowed but possibly user actions in order to avoid or limit liability. Ultimately, an approach along those lines could fundamentally impact the control users have on their computer. It could also result in more and more closed platforms and a potential situation where one dominant provider could dictate what can be installed and may limit the choices of consumers to "approved content". This could have a negative impact on competition in the market and risks creating monocultures in information security terms which, as explained to the Committee in our written and oral evidence, could create a single point of failure across the Internet's infrastructure. As a result there is real concern that the introduction of vendor liability could have the unintended consequences of reducing consumer choice and negatively impacting the level of information security that users currently enjoy. If vendors have to absorb product liability in their business models then the current innovation environment of open and interoperable platforms will be radically shifted.

Symantec remains supportive of the overall objectives of the Committee in trying to support Internet users and ensure there is an adequate level of protection for users against online threats. The Government's recognition that the debate around vendor liability should not prevent innovation in the market or lead to a reduction in the quality of software is welcomed. However, it is argued that by following a legislative path discussed by the Committee that may lead to the introduction of vendor liability could very well result in the situation that the Government agrees must be prevented.

March 2008