THE GOVERNMENT REPLY TO
THE FIFTH REPORT FROM THE
HOUSE OF LORDS SCIENCE AND
TECHNOLOGY COMMITTEE
SESSION 2006-07 HL PAPER 165

Personal Internet Security

Presented to Parliament by the Secretary of State for the Home Department by Command of Her Majesty October 2007

Cm 7234 LONDON: THE STATIONERY OFFICE £5.00

THE GOVERNMENT REPLY TO THE FIFTH REPORT FROM THE HOUSE OF LORDS SCIENCE AND TECHNOLOGY COMMITTEE SESSION 2006-07 HL PAPER 165

PERSONAL INTERNET SECURITY

Introduction

The House of Lords Science and Technology Committee published its report of session 2006-07, on personal internet security on 10 August 2007. This Command Paper sets out the Government's response to the conclusions and recommendations in that report.

The Government welcomes the report, and recognises the detailed work that the Committee has carried out to highlight the issues surrounding the use of the internet and its impact on the welfare of users. It welcomes this contribution to the development of thinking on this increasingly important subject and believes the Report has usefully taken stock on the views of the relevant stakeholders and has fostered informed debate around its conclusions.

The Government does not agree with the implication within the report that the public has lost confidence in using the internet. The continuing increase of trading on the internet, with year-on-year growth of 80% in some areas, does not support such a view. The explosion in user generated content and the opening of new and varied forms of social interaction through the internet also underlines the interest in and - if not absolute confidence – then an acceptable level of comfort with the technology.

The Government recognises the dangers of complacency against this background of continuing success. Although the number and sophistication of security threats has risen over recent years the Government believes that this has to be viewed in the context of the dramatic increase in internet usage. As such, we would refute the suggestion that the public has lost confidence in the internet and that lawlessness is rife.

The Government takes seriously all crime committed by use of the internet and agrees with the Committee that confidence in the internet is vital. However, we also feel there is an unwarranted suggestion that its only response to the problem is to regard it as a personal responsibility of the user to take necessary precautions. It is true that the user should be aware and both take precautions and behave responsibly. But this is not the only way to improve personal internet security and the Government's written and oral evidence supports the Committee's conclusion that this is a shared responsibility. It therefore welcomes many of the recommendations in the report and notes, in particular, the support for initiatives like Get Safe Online as an important route to encouraging awareness and personal responsibility, which we continue to believe is a key component in ensuring confidence in the internet. Legislation will be kept under review but the Government does not consider that imposing additional burdens on business is the best way forward.

The Government will consider the proposals to create a law enforcement unit to tackle crimes involving computers. This will be done in conjunction with the proposals for the development of the National Fraud Reporting Centre, and with regard to the needs of other agencies.

The Government has considered all the evidence presented to the Committee, and these views together with the conclusion and recommendations contained in the report are valuable to the ongoing debate about internet security.

The Government's Response to the Committee's Conclusion and Recommendations

The Internet and Personal Security

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 ecrime.

The Government actively encourages discussions between all groups, and there is considerable contact between Government departments and industry. That said, we are currently working towards setting 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 do not see that there is a need for any such group to devise a "classification scheme for the recording of all forms of ecrimes" because we take the view that prosecution should be based on the offence, and not on the tools used in committing that offence. Crimes committed using computers as the medium, or as part of a specific crime, are standard offences that are facilitated by new technology, rather than new types of offence. These offences are recorded under the specific offence or Act.

The Computer Misuse Act 1990 covers offences relating to unauthorised access to computers, and the alteration of damage or data stored in them. Prosecutions under the Act are recorded.

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.

All Research Councils have an interest in internet security, but as a subject area the technology aspects fall to the Engineering and Physical Sciences Research Council (EPSRC) and the social and economic aspects to the Economic and Social Research Council (ESRC). The Councils welcome the observation that there is a need for major multidisciplinary research in this area.

EPSRC and ESRC have already established links to encourage, and mechanisms to fund, multidisciplinary research that spans the boundary between EPSRC and ESRC. In addition, they are currently partnering with the Technology Strategy Board (TSB), under its Network Security Innovation Platform, to deliver a new activity in Ensuring Privacy and Consent (EPAC). The joint research programme will enable UK industry, universities, local authorities and other research and technology organisations to work in collaboration to address key research challenges in ensuring privacy and consent in next generation systems. The programme is being undertaken in association with the Home Office and the Identity and Passport Service. Further details can be found at: http://www.technologyprogramme.org.uk/site/ip/nsip/.

In addition, Research Councils are considering a possible cross-Council collaboration entitled the 'Digital Economy'. Key Councils are EPSRC and ESRC, although the Science and Technology Facilities Council (STFC), the Natural Environment Research Council (NERC) and the Arts and Humanities Research Council (AHRC) are also engaged. The programme will focus on the transformational ability that Information and Communications Technologies (ICT) can have on business, recognising the broad range of technical, research and social issues that need to be addressed to enable rapid delivery of new capabilities. This will include significant elements of work relative to this area. The programme will focus on industry led application areas, building multidisciplinary consortia to address grand challenges. The scale of the activity is dependent on the outcome of the current Spending Review.

We note, but do not accept, the Committee's view that security researchers are at risk of being criminalised because of the recent amendment to the Computer Misuse Act (CMA), namely the new section 3A offence which criminalises the making, supplying or obtaining of articles for use in offences under section 1 or 3 CMA. We believe that it is right that those in the legitimate IT security sector, who make, adapt and supply tools as part of their daily work should have confidence that the new offence will be used appropriately and be assured that their practices and procedures fall within the law. The CPS is currently drafting guidance on how the new section 3A offence will be dealt with and this will be issued shortly.

The Network

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

This recommendation is largely technical and as such falls mainly within the remit of the EPSRC. The EPSRC supports a large portfolio of research in this broad area, funding 78 grants at a value of £11.7 million since 2000. The support of fundamental, underpinning research through open responsive mode continues to be a priority for the EPSRC. In addition, it supports the development and networking of the community that underpins this area. In the last year, EPSRC supported network activities in 'Next Generation Wireless Networks' and 'Next Generation Networking' through open responsive mode. It also sponsors travel for overseas engagement and speakers or other elements of relevant conferences or workshops with the community.

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

The Government certainly agrees that a large number of stakeholders need to have a clear focus on the need for personal internet safety and, indeed, this is more than a distributed responsibility as the actions of one internet user or participant can impact on the welfare of others. Our evidence to the Committee highlighted the considerable work that is going on across Government to improve the security of the nation's information infrastructure. This work is led by the Cabinet Office and involves a co-ordinated effort by the Cabinet Office's Central Sponsor for Information Assurance, the Centre for Protection of the National Infrastructure and the Communications and Electronic Security Group. That work has taken a strategic view of what actions the Government should be taking and we acknowledged the important range of activities that are going on across Government to address personal internet security issues.

This work includes:–

- Formulating an information assurance strategy for Government; this underlines the importance of improved performance based on a risk-based approach to the protection of information assets. The strategy acknowledges the importance of non-Governmental stakeholders contributing to the strategy's goals;

- Efforts to improve the quality of software and services; CPNI, Cabinet Office and the Department for Innovation, Universities and Skills (DIUS) all have activities to engage with software vendors to assist with the identification and remediation of vulnerabilities, promote testing arrangements to give confidence in the use of software and hardware security products and to more generally promote good software design.

- Engaging with service providers; BERR, Home Office and other Government Departments are actively pursuing ideas with the Internet Service Providers as to how they might work even more closely with their customers to prevent harm to customer equipment and prevent those customers causing harm to the networks and other users. This will necessarily embrace issues around harmful content.

- Outreach to business and home users: Recognising that many problems can be avoided by appropriate actions by users, the Government has a long history of direct engagement with business on security measures and this has been enhanced by a Knowledge Transfer Network that is creating a new approach to identifying and disseminating best practice. Outreach to school age children has been significantly increased this year with the addition of Internet safety and security in secondary schools curriculum at Key Stage 2.The success of Get Safe Online, a public private initiative, has increased the awareness of home users and micro businesses of what they can do to prevent falling foul of security problems.

The Government can therefore accept the spirit of the recommendation in that we must continue to deepen our understanding of the issue of personal internet security and what can be done to improve it, and indeed has taken some significant steps on this in recent years. We would not, however, accept the view of the Committee that the Government has taken a narrow view of this problem in the past.

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 an obligation will be placed upon 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.

The Government accepts that the ISPs have an important role in preventing security problems for users. ISPs cannot remove all their problems but there are things they can do to both optimise the ability of their networks to filter bad traffic – accepting that there are technological limitations to this – and have a relationship with their users that promotes responsible behaviour. There are many ISPs that have shown innovative and committed approaches to solving these problems but we agree that there is a need to both look for a way of identifying what a customer has a reasonable right to expect and ensuring that ISPs who meet that expectation can clearly indicate

it. This work will clearly need to consider preventing the transmission of bad traffic from customer machines into the ISPs' networks. The Committee took evidence that this is happening and the practice of isolating such machines from the network is already happening to a certain extent. The potential for increasing this practice will need to be explored.

Whether this should be a kite mark – a mechanism more closely associated with products rather than services – or some other mechanism must be for the industry to decide. The Government has indicated its willingness to work with the industry to promote greater consumer confidence in the contribution that ISPs can make to their online security. This work should be informed by and build on the recently announced initiative on child protection online and existing industry initiatives such as the Internet Watch Foundation and relevant work by the Internet Service Providers Association and others. It should also acknowledge the value of the work taken forward by the CSIA on establishing and giving market recognition of the veracity of claims about products and services through the Claims Testing Mark.

At this stage, we see no need to commit to a regulatory underpinning of this approach. It is clear that the review of the EU regulatory framework for communications providers will address security and consumer issues in greater depth. It would be unwise to propose regulatory change before any revised requirement to meet European legislation has been clarified.

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.

The Government simply cannot implement selectively those parts of European legislation that give protections to ISPs who act as mere conduits. It is, in any case, not true that the protection is absolute and it is possible for an ISP to be compelled by, for example, a court order to take action. Moreover, it is by no means clear that if the mere conduit protection were removed that it would then be possible for third parties harmed by infected machines to recover damages from an ISP.

There is an assumption in the report that ISPs do not take appropriate action against compromised machines that are serviced by their networks. We do not believe that this is completely true and, indeed, evidence to the Committee made clear that the leading ISPs set user terms and conditions that enable them to isolate machines identified or notified as causing problems. It is in the interest of the ISPs to take such actions. As we say elsewhere in this response, we believe that the 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.

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.

Ofcom are concluding a second round of consultation on the provision of access to the 999 service by VOIP providers. The Government agrees that we need the greatest possible access to the 999 service but believe that it is for Ofcom, acting as the independent regulator, to agree the best solution taking account of the technology and business models deployed in the market.

Appliances and Applications

8. We therefore recommend that the Government explore, a European level, the introduction of the principle of vendor liability with the IT industry.

The Committee took considerable evidence on the problems associated with changing the liability model for software licensing and this highlighted the arguments both for and against such a move, for example the counter-arguments to the view that changes in liability would incentivise the production of better software. The Government considers that there is scope for further discussion at the European level and this is already taking place as part of the ongoing Review of the Consumer Acquis. This debate should consider how to both improve the reliability of software and protect the interests of consumers while not reducing the quality of software available on the market or the incentives to innovate.

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 can accept that new forms of online activity, including the expansion of supply chains to include systems in a multitude of jurisdictions, poses new challenges for data protection enforcement. We do not accept that the incidence of loss of personal data by companies is on an upward path and we do not accept that the Government is indifferent to the problem. The Government believes that the market incentives provided by the impact of adverse publicity surrounding breaches of security are powerful drivers to apply appropriate protection. The Government also believes that the current legislative and enforcement regime surrounding personal information is proportionate and provides a strong incentive to appropriate action by companies. The Government agrees that it cannot prescribe the technologies or processes that should be deployed to protect information but we accept the spirit of the Committee's recommendation in part. We accept that the business models being adopted by companies whereby personal information is processed by sub-contractors in various jurisdictions is proving a challenge in both management terms and in relation to the underlying principle of European legislation that equivalence of protection should be ensured. A recent report by the Information Age Partnership and BERR pointed to the need to look at this problem and move towards solutions that work with the emerging global market in online services.

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.

The Government does not support this recommendation. 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. In practice, banks normally reimburse cardholders who have been genuine victims of online card fraud – however banks cannot be expected to reimburse those who have been negligent with their card and/or card details. Neither should banks be expected to reimburse cardholders who may have been complicit in the fraud.

Victims of online card fraud are protected by the Banking Code which says that:

- If someone else uses your card details without your permission for a transaction where the cardholder does not need to be present, you will not have to pay anything.

Moreover, not all electronic fraud will be fraud against a payment card. It is not clear what exactly the report means by "electronic fraud". Other online frauds may include:

- frauds conducted via e-mail (eg advance fee type fraud, boiler room fraud)
- frauds connected with internet auctions – but not necessarily taking place on the internet auction website (for example "second chance" type offers).

In these cases, banks cannot be held responsible for lack of security, nor can they be held responsible for reimbursing losses to victims.

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.

The Government provided evidence to the Committee that recognised that the move towards breach notification laws in other jurisdictions was an interesting development. We are, however, clearly not so convinced as the Committee that this would immediately lead to an improvement in performance by business in regard to protecting personal information and we do not see that it would have any significant impact on other elements of personal internet safety. The experience in the United States has yet to be fully analysed but there is a strong body of opinion that doubts whether there has been significant differences to corporate behaviour and may, in fact, have desensitised consumers to security issues and undermined confidence in the internet as a business medium. It has to be remembered that the US does not have the same legal framework in respect of privacy and the state laws on data breach have been an attempt to provide market incentives as an alternative to imposing such a framework. We will continue to observe the US experience and consider whether we need to find more formal ways of ensuring that companies do – as a matter of routine – contact the Office of the Information Commissioner when problems arise. This enables a proportionate response to be taken and ICO acknowledge that there are occasions when notifying consumers of a breach of security might not be

appropriate. Such discussions also enable a discussion to take place about precautions taken and how they might be improved.

We agree with the Committee's conclusions that there appears no obvious justification to apply such requirements to the communications providers in isolation.

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

- *Workable definitions of data security breaches, covering both a threshold for the sensitivity of data lost, and criteria for accessibility of that data;*
- *A mandatory and uniform central reporting system;*
- *Clear rules on the form and content of notification letters which must state clearly the nature of the breach and provide advice on the steps that individuals should take to deal with it. (5.56)*

We fully agree with the Committee that, should we eventually go down the route of introducing a data security breach notification requirement, these are important points to take into account to make it fit for purpose.

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.

As noted above, the Government believes that the current enforcement regime for data protection is fit for purpose. The Ministry of Justice has regular contact with the Office of the Information Commissioner and the powers available to the Commissioner are discussed regularly in that context. The effectiveness of the enforcement regime is covered in the annual report that the Commissioner is required to make to the Government.

Using the Internet: The Individual

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 recognises the need for high-level political support and fully endorses the need to recruit additional sponsors. In the past two years the Get Safe Online initiative has received high-level ministerial support from Tony Blair, John Hutton, Jim Murphy and Pat McFadden. The Central Sponsor for Information Assurance (CSIA) at the Cabinet Office works with existing, previous and potential sponsors to seek support from their senior management and will seek to gain senior ministerial involvement in the initiative as appropriate.

The Government appreciates the attractiveness of a single portal devoted to personal internet security rather than numerous sites, and this is in line with the government website rationalisation objective already being pursued under the Transformational Government agenda. CSIA will work with Direct Gov and Business Links in rationalising the approach to providing internet safety information to customers.

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

We understand that Ofcom intend to make a full reply to the Committee on points addressed to them. We also understand that the recommendation of the Committee has led to discussion between Get Safe Online and Ofcom and areas for closer collaboration and mutual support have already been identified. We welcome this and trust that dialogue will continue and the relationship between GSOL and Ofcom will deepen over time. We believe that Ofcom's reply will draw attention to their strategic focus on content management and content information and to its governance model for determining which Media Literacy initiatives it can fund.

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

As noted above, Ofcom will reply to these points and we believe that they will rightly note the success of the initiative on content control software for parents and the progress on codes of practice on networking sites. The Government believes that the testing of security software is something that has been happening for many years through the Common Criteria arrangements. The Government would draw the Committee's attention to its recent initiative on establishing a Claims Tested mark which provides assurance to purchasers of security software and services that the claims made for the product in terms of functionality have been independently tested for their veracity.

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.

Becta (the British Educational Communications and Technology Agency) is working with key partners, Childnet International, the Home Office and the Department for Children, Schools and Families (DCSF) on the issue of educating parents about the dangers of the internet. DCSF have worked with Childnet International to distribute one million CDs that support parents in understanding the dangers of the internet. Approx 200,000 of these have been distributed through the retailer PC World and information has been preinstalled on computers issued through the Computers for Pupils initiative.

Becta chairs a sub-group of the Home Secretary's Taskforce for Child Protection on the Internet education that is looking at this particular issue and will be discussing potential strategies with both the Home Office and the DCSF. The DCSF 'Staying Safe' consultation proposes a potential 'safety' campaign which would include wider safety issues but would also include online safety.

Policing the Internet

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.

We believe that because Section 3 of the Computer Misuse Act 1990, as amended by the Police and Justice Act 2006, allows us to prosecute someone who obtains, is selling or uses an illegal botnet, we can meet the concerns of the Committee.

Our supplementary memorandum to the Committee set out the legal position as we see it. However, it may be useful to also add that the problem has always been that illegal use is being made of articles that have a legitimate use. A small collection of remotely controlled software (and therefore identical in nature to bot software) may be held, for example, for security testing purposes or academic research, and should not necessarily be criminalised. The CMA, as amended, has not therefore criminalised lawful position of bots for such purposes.

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.

There is an overlap between the Fraud Review National Fraud Reporting Centre (NFRC) proposal and the proposed ACPO national ecrime unit to tackle crimes involving the use of computers. A working group has drawn up a full business case for the NFRC for consideration as part of the CSR process. We believe it is important that we ensure that all efforts to combat crimes online are co-ordinated and as such we will consider this recommendation in the context of the fraud review.

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.

The changes to Police reporting and recording procedures for plastic and cheque fraud cases was made to reduce bureaucracy for account holders, the financial industry and the Police. Detailed discussions and consultations took place between the Association of Chief Police Officers, Police forces, Association of Payment Clearing Services and the Home Office where agreement was reached before this change was introduced on 1st April 2007. Where financial institutions refund monies lost by fraud to individual account holders, it is a matter for financial institutions to report these cases direct to newly created Single Points of Contact within Police forces. Where account holders are not refunded they retain the ability to report these matters directly to the Police, where crimes should be recorded.

For statistical purposes APACS own figures show there were nearly 2.3 million plastic card fraud transactions for UK issued cards in 2006. The corresponding figures for police recorded crime for plastic card and cheque fraud for 2006/07 were just over 59,000. The process prior to 1st April 2007 involved an account holder generally notifying their financial institution in the first instance about suspected fraudulent transactions. If the account holder also notified the Police, the Police would write to the financial institution and seek confirmation of the fraud before a crime would be recorded. If the financial institution did not confirm the crime then Police would normally retain this information as an 'incident' as opposed to a crime. Where the financial institution did respond the Police would make a decision in relation to which Police force should record the crime based on the location of the offence, as confirmed on the schedule of usage supplied by the financial institution. If this was different from the force that the account holder had originally reported their suspicions to, the crime would need to be transferred.

The new Rules from 1st April allow financial institutions to directly contact single points of contact within forces to quickly and accurately report and have recorded allegations of crime. There is no requirement for individual account holders to deal both with the financial institution and also repeat the same facts to the Police for a crime to be recorded where account holders have already been refunded monies by the ultimate victim who is the financial institution. The Home Office will continue working with ACPO, individual forces and APACS to ensure that any issues in connection with the new system are addressed to the satisfaction of users.

The changes from 1st April will significantly reduce police bureaucracy in this area without any loss of effectiveness in dealing with frauds or any degradation of the service provided to victims and provides a better basis for the police to work in partnership with financial institutions to tackle fraud.

21. We therefore recommend the establishment of a network of computer forensic laboratories, under the aegis of the proposed ACPO national ecrime 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 ecrime Unit, without waiting for the private sector to come forward with funding.

The Government takes seriously the threat of all crimes involving the use of computers. We know that such crime is not a problem that sits comfortably within local policing structures, and that historically most forces have underinvested in their capacity to respond effectively to it. We therefore believe that national co-ordination would bring some obvious benefits to the policing of these crimes. As discussed in recommendation 19, the cross-Government Fraud Review, which reported last year, similarly recommended the creation of a National Fraud Reporting Centre. We believe it is important that we ensure that all efforts to combat crimes online are co-ordinated.It is essential that any structure developed must meet clearly defined needs to allow an effective response, this means consideration of all the issues relating to crimes involving the use of computers and how best to tackle them in a coherent fashion. This will, in turn, lead to decisions on the infrastructure that will be needed to support that.

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 United Kingdom 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 ecrime.

In our evidence to the Committee, we discussed the fact that we remain committed to ratifying the Council of Europe Convention on Cybercrime, which we signed in 2001. We have recently legislated, in the Police and Justice Act 2006, to reform the criminal law to ensure that the Computer Misuse Act 1990 is fully compliant, and we will ratify the Convention as soon as possible. However, we will not do so before we implement the Computer Misuse Act changes in April 2008.

With regard to Article 25 of the Convention, we are satisfied that provision for mutual legal assistance under the Crime (International Co-operation) Act 2003 is sufficient to respond to requests for help from other countries relating to crimes perpetrated using computers. However, we keep these matters under constant review to determine whether any further measures are necessary and any improvements may be made.

23. We recommend that the Government take steps to raise the level of understanding of the Internet and ecrime across the court system. In particular:

- **In the context of the prevalence of identity theft and online card fraud, we urge the Government to issue new guidance to the courts, including magistrates' courts on the reliability of unsupported credit card evidence as an indicator of guilt.**
- **We recommend that the Government review the availability to the courts of independent specialist advice of internet-related crime.**
- **We believe that the sentence should fit the crime. The nature of ecrime 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 review in recognition of these realities.**

The credibility of evidence is a matter for the courts to determine. Our adversarial system enables both parties to test evidence through cross-examination. It would not be appropriate for the Government to issue guidance to the courts on this matter. However, we have passed the report to the Judicial Studies Board for their consideration.

The Government believes that the tried and tested arrangements for admitting expert opinion evidence provide a satisfactory basis for the admission of specialist advice in criminal proceedings. The law already enables expert opinion evidence to be submitted in court, where appropriate, by the prosecution or defence. As the report recognises, it is difficult to reconcile the concept of an impartial adviser with the principle of adversarial proceedings.

Printed in the UK by The Stationery Office Limited
on behalf of the Controller of Her Majesty's Stationery Office
ID5677905 10/07 19585 380917

Printed on Paper containing 75% recycled fibre content minimum.

Published by TSO (The Stationery Office) and available from:

Online
www.tsoshop.co.uk

Mail, Telephone, Fax & E-mail
TSO
PO Box 29, Norwich NR3 1GN
Telephone orders/General enquiries: 0870 600 5522
Order through the Parliamentary Hotline *Lo-call* 0845 7 023474
Fax orders 0870 600 5533
Email customer.services@tso.co.uk
Textphone 0870 240 3701

TSO Shops
16 Arthur Street, Belfast BT1 4GD
028 9023 8451 Fax 028 9023 5401
71 Lothian Road, Edinburgh EH3 9AZ
0870 606 5566 Fax 0870 606 5588

The Parliamentary Bookshop
12 Bridge Street, Parliament Square,
London SW1A 2JX

TSO@Blackwell and other Accredited Agents

ISBN 978-0-10-172342-8

9 780101 723428