THE GOVERNMENT RESPONSE TO THE FIFTH REPORT FROM THE HOME AFFAIRS COMMITTEE SESSION 2013-14 HC 70:

E-crime

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

October 2013

Cm 8734 £6.25

THE GOVERNMENT RESPONSE TO THE FIFTH REPORT FROM THE HOME AFFAIRS COMMITTEE SESSION 2013-14 HC 70:

E-crime

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

October 2013

Cm 8734 £6.25

Any enquiries regarding this publication should be sent to us at:
jon.williams37@homeoffice.gsi.gov.uk

Cyber Crime Team,
Home Office,
2 Marsham Street,
London,
SW1P 4DF

ISBN: 9780101873420

Printed in the UK by The Stationery Office Limited
on behalf of the Controller of Her Majesty's Stationery Office

ID 2596713 10/13 33669 19585

Printed on paper containing 75% recycled fibre content minimum

Home Affairs Committee Report on E-crime: Government Response

Introduction

The Government is grateful to the Home Affairs Committee for its report "E-crime" (HC 70), published on 30 July 2013. This document is the Government's response to that report.

The internet is revolutionising society by driving economic growth and giving people new ways to connect and co-operate with one another. However these opportunities also bring with them new threats from criminals, other nation states, terrorists and online activists.

The Government's National Security Strategy, published in 2010, ranked UK cyber security, of which cyber crime is an element, as a tier 1 national security priority. The Government committed £650 million over four years to the transformational National Cyber Security Programme (NCSP) to bolster its cyber defences, and a further £210 million has now been allocated to the programme for 2015/16.

In November 2011, the Government published its National Cyber Security Strategy which set out how the UK will support economic prosperity, protect national security and safeguard the public's way of life by building a more trusted and resilient digital environment. The Government's approach for tackling cyber crime (objective one of the National Cyber Security Strategy) is a comprehensive strategy for meeting the threat, increasing the capability to tackle it and strengthening the law enforcement response to it. The UK Government will continue to liaise with the devolved administrations as necessary on this work.

Tackling cyber crime is also an important priority within the Government's Serious and Organised Crime Strategy that was published on 7 October 2013; the same day that the new National Crime Agency was launched. The National Cyber Crime Unit, which is part of the National Crime Agency, will transform the UK's capability to tackle cyber crime.

Reporting and recording cyber crimes:

HAC 1: Crimes that have been transformed by the internet and those unique to electronic networks should continue to be defined and recorded as e-crime. This will enable the police to develop an appropriate level of sophisticated technical resource to respond to these crimes. (Paragraph 12)

1. The Government acknowledges HAC conclusion 1. A single national reporting centre has been established for financially-motivated cyber crimes through Action Fraud. This receives reports of both computer-dependent crimes (those that can

only be committed through the use of computers, computer networks or other forms of information communication technology (ICT)) and computer-enabled crimes (traditional crimes that are increased in their scale or reach through the use of computers or other forms of ICT). These crime reports are analysed by the National Fraud Intelligence Bureau (NFIB) of the City of London Police who identify linkages between crimes and disseminate then for the appropriate law enforcement response.

HAC 23. We welcome the online Action Fraud reporting function. We recommend that a clear link to the Action Fraud website is placed on websites where people are likely to experience attempted fraud or visit when they believe they have been a victim of online fraud such as police forces, banks, email providers, trading standards. (Paragraph 82)

2. The Government supports recommendation 23 and acknowledges the HAC support for having a centralised reporting function. It is a key priority to raise awareness this by ensuring as many organisations as possible direct potential victims to it.

HAC 24. Current recording practices are inadequate to give an accurate picture of the extent to which reported crime is committed over the internet. We recommend the introduction of an additional field on crime reporting forms to indicate whether or not there was digital evidence relating to a crime. This would help the police to understand the extent of the problem they were facing and to make sure they have the appropriate resources in place. (Paragraph 83)

3. The Government accepts HAC recommendation 24. A large numbers of crimes reported to local police forces may now have a "computer" element, but the computer itself may not have been integral to the commission of the crime (such as harassment). The Home Office is exploring ways to improve the ability to identify such crimes within police recorded crime figures. The Home Office has developed a 'cyber flag' that will enable forces to highlight, within police recorded crime figures, which crimes which have taken place online. This flag is running on a voluntary basis only during 2013/14 and will be subject to wider consultation to determine if it should become mandatory for 2014/15.

HAC 25. We are very concerned that there appears to be a 'black hole' where low-level e-crime is committed with impunity. Criminals who defraud victims of a small amount of money are often not reported to or investigated by law enforcement and banks simply reimburse victims. Criminals who commit a high volume of low level fraud can still make huge profits. Banks must be required to report all e-crime fraud to law enforcement and log details of where attacks come from. The perceived untouchable nature of these low-level criminal acts is exemplified by the adverts RSA noted on Facebook advertising 'fraud as a service'. (Paragraph 84)

4. The Government does not accept HAC conclusion 25. Low-value fraud is often part of wider criminal activity targeting many potential victims. Whilst a single incident of low-value fraud might not be investigated by the police given its value, when put together with other linked crimes, this low-level fraud can result in a high level of harm. This is why Government has supported the roll out of the Action Fraud service, so that NFIB can analyse reports of fraud received from a number of sources including Action Fraud and the payments industry. Through this analysis, links between seemingly unconnected crimes may be detected. In this way it is possible to identify high-volume, low-value frauds where there are common operating models and many victims, which can result in targeted enforcement activity by the police against the group involved. The NFIB will work to monitor the investigations which take place as a result of these disseminations to ensure that these networked low-level frauds are pursued.

5. Businesses also provide information packages to NFIB which can also be used by law enforcement agencies to tackle this type of fraud. The Government is working closely with industry to encourage them to report all instances of low-level fraud and cyber crime to ensure that law enforcement agencies are able to see the full picture.

Policing capabilities:

HAC 2. The ever-increasing incidence of the use of the internet in some form in traditional crimes indicates the futility of special categorisation for such offences. We recommend that more police officers are trained in digital crime detection and equipped with digital forensic skills. These should become standard skills for officers undertaking relevant investigations. (Paragraph 13)

HAC 17. However commitments to improve mainstream skill levels have been around for years and practice has not so far matched rhetoric. We hope to see clear evidence that the work promised is being undertaken and clear benchmarks to measure if skills are improving. (Paragraph 60)

HAC 18. We welcome the development of specialist Digital Scenes of Crime and forensic officers and note that the search and seizure of digital material should only be done when it is proportionate. (Paragraph 64)

6. The Government accepts HAC recommendation 2 and acknowledges conclusions 17 and 18.

7. The National eCrime Programme, funded through the National Cyber Security Programme, seeks to increase law enforcement's capacity and capability in relation to cyber crime through the provision of additional training and capability to both specialist and mainstream police officers.

8. The training of police officers is being enhanced to make officers more aware of how to utilise new technologies when investigating crime. This work has been done in conjunction with the College of Policing which now holds the responsibility for delivering training to law enforcement officers.

9. Twelve existing courses aimed at new officers and new-to-role detectives have been reviewed and redeveloped, creating a cyber crime content. These will be rolled out to forces over the next six months. A new e-learning package has been developed and rolled out giving a foundation level of understanding of cyber for all officers and staff. Since its launch in April 2013, it has been delivered to over 2,815 officers and staff. Additionally a week long course, specifically about cyber crime and associated technology, is being developed for existing staff, and will be delivered to up to 5,000 officers in the next 18 months.

10. Work is also ongoing to ensure that training across law enforcement takes proper account of how communications technology, the communications industry and communications usage are changing and how this might affect criminal behaviour. In the past three years, the Communication Capabilities Development programme has allocated funding for a wide range of initiatives to make more effective use of communications data, including training for analysts and investigators. A five-day course for investigators and analysts has been delivered to over 7,000 police officers and staff since October 2010 with a further 1,200 places made available through the College of Policing in 2013/14.

HAC 5. Commissioner Leppard told us that a quarter of the 800 specialist internet crime officers could be axed as spending is cut. We agree with him that this is a very worrying trend. At a time when fraud and e-crime is going up, the capability of the country to address it is going down. (Paragraph 24)

HAC 16. We welcome the establishment of regional hubs to support and develop local capacity and skills. Mainstreaming e-crime investigative skills throughout the police force is key to improving capacity across the board. We welcome the work currently being undertaken by Police Central e-crime Unit and others in this area. (Paragraph 59)

11. The Government does not agree with HAC conclusion 5 that the capability within policing to tackle cyber crime is diminishing. The Government welcomes HAC conclusion 16 - through the investment of the National Cyber Security Programme, three regional cyber policing hubs were established as pilots in the North West, East Midlands and Yorkshire and Humber regions. These new specialist policing capabilities have been established with the technical skills to tackle technologically-advanced criminals outside London and to build skills locally. In their first year of operations, these hubs provided support to both local

and national law enforcement partners on cyber operations. Now, extra funding is being provided in 2013/14 to expand regional cyber operations with the aim that every Regional Organised Crime Unit should have a dedicated cyber unit.

National Crime Agency:

HAC 12. We welcome the steps being taken by Government to bring together different cyber crime units into the NCA to form a single National Cyber Crime Unit. This rationalises the current confusing plethora of different agencies and police organisations involved and should enable a more co-ordinated approach, strong strategic leadership and development of the elite level of skill required to tackle this cyber war. (Paragraph 53)

12. The Government acknowledges HAC conclusion 12 and welcomes the Committee's endorsement of the steps being taken to unify the national law enforcement response to cyber crime. The National Cyber Crime Unit is more than a simple merger of its precursors. It will transform the UK's capability to fight cyber crime by: providing a highly specialised investigative response, nationally and internationally, to the most serious incidents of cyber crime; working proactively to eliminate criminal opportunities and create a hostile environment for cyber criminals; assisting law enforcement to tackle high-level cyber-enabled crime; and also driving the up-skilling of law enforcement and building stronger partnerships to cut crime.

HAC 31. We are concerned to note the Minister's assertion that off the shelf hacking software is increasingly available to untrained criminals and recommend the Government funds a law enforcement team which is focused on disrupting supply. (Paragraph 106)

13. The Government accepts HAC recommendation 31. One of the key objectives of the new National Cyber Crime Unit is to work proactively to eliminate criminal opportunities and create a hostile environment for cyber criminals. This includes disrupting the supply of hacking software and other tools available online, alongside intervention operations.

HAC13. We were concerned however that the National Fraud Reporting Centre and the National Fraud Intelligence Bureau based in the City of London Police were not being transferred into the NCA. In our view it makes sense to concentrate the national reporting, investigative and intelligence structures for e-crime in one organisation. We were surprised at the decision given the formation of the new economic crime command in the NCA and given we were told that the UK was the main online target of gangs in 25 countries. (Paragraph 54)

14. The Government does not agree with HAC conclusion 13. The Government believes that it is appropriate to retain the separation between the remits of the National Crime Agency and the City of London Police. The City of London Police's National Fraud Investigation Bureau, informed by the national reporting function for fraud and cyber crime, is best placed to carry out the analysis of crime reports and disseminate packages to the relevant law enforcement agency or police force for investigation. It will work closely with the National Crime Agency's intelligence hub to ensure that intelligence is being shared effectively and opportunities to tackle cyber criminals are being suitably identified and acted on, The National Crime Agency sits at the heart of law enforcement and leads the fight against serious and organised crime. With its Economic Crime Command (ECC) and the new National Cyber Crime Unit, the National Crime Agency has a lead crime-fighting role in relation to economic and cyber crime. Additionally, it has the authority to coordinate and task the overall national response to serious and organised crime. The NCA is a crime-fighting agency that works closely with police forces such as the City of London Police; it is not intended to be a crime reporting organisation.

HAC 14. The Committee's report on grooming published earlier this year found that sexually exploited children were still being failed by statutory agencies, and the recent court cases of Mark Bridger and Stuart Hazell have highlighted the role of online indecent images in child abuse. An NSPCC Freedom of Information request revealed that five police forces alone had seized 26 million indecent child images and 2,312 people were arrested for such offences last year. CEOP also estimates there are 50,000 indecent child images on Peer2Peer networks. We are therefore alarmed that CEOP is having its budget cut by 10% over 4 years, its experienced Chief Executive is leaving and it could lose its laser-like focus when merged with the NCA. (Paragraph 55)

15. The Government does not accept HAC conclusion 14. Government funding for the Child Exploitation and Online Protection Command of the National Crime Agency was higher in 2012/13 (£6.381 million) than it was in 2009/10 (£6.353 million). The CEOP budget has effectively been protected in cash terms since 2011/12 and there are now more people working in CEOP than at any time in its history.

16. Being a distinct Command in the NCA will bring advantages to CEOP. Its existing operating principles have been preserved as agreed when the Plan for the NCA was published, including its innovative partnerships with private and voluntary sectors. It will also gain access to more capacity to deal with complex cases of child sexual exploitation and abuse. It will gain greater resilience for front-line operational services and benefit from support from other NCA specialist functions. Its influence, as part of the national leadership the NCA will have across law enforcement, will be enhanced. The Crime and Courts Act 2013

places a statutory duty on the NCA to safeguard and promote the welfare of children in England and Wales, which means that all officers, not just those directly involved in child protection, will receive mandatory training on safeguarding children. This means that every one of over 4000 officers will have a legal duty to safeguard and promote child welfare so will be able to protect even more children from harm.

International:

HAC 19. We were alarmed to hear from police witnesses that they often experienced difficulty in retrieving data from sites based abroad. We hope that such companies will adopt a more constructive attitude going forward and be willing to engage with public authorities. They reap huge financial benefits from the public entrusting them with their data and they should be willing to be open and accountable for the actions they take with it. (Paragraph 69)

17. The Government supports HAC conclusion 19. It is important for companies to engage with the authorities in order to provide data requested from abroad. The Government is working to make the most effective use of the routes in place, including by improving the awareness of UK law enforcement agencies relating to communications data, improving relationships with overseas communications service providers, and by making further use of police-to-police cooperation in accordance with the Budapest Convention on Cybercrime. SOCA's Overseas Liaison Officers work with the private sector in this area and have been able to deliver tangible results on a number of cases. The NCA took over this overseas network on October 7. As explained at paragraph 16, the new Agency will further strengthen the ability (and duty) of overseas officers to take action against those who seek to harm children.

18. A number of these points were raised during the Parliamentary scrutiny of the draft Communications Data Bill, and the Government is continuing to consider how to address a number of these challenges. Legislation may be required to do this.

19. The Government also recognises that some of the mutual legal assistance process must improve, particularly the transmission of requests for digital evidence. We are looking into what the UK can to do to speed up transmission of requests abroad, and also how the domestic process for issuing a request can be made more efficient.

HAC 20. The international scope of e-crime provides a strong argument that the UK should focus on increasing cooperation between police forces in other states and making these mechanisms as effective as possible. As the proportion and volume of crime with an online element increases, we expect

more police investigations to straddle international boundaries, and more evidence relating to the offences against the UK and its residents to be located in overseas jurisdictions. (Paragraph 72)

20. The Government supports HAC conclusion 20. It is essential for the UK to cooperate with partners overseas to tackle cyber crime and this is a key element of both the Cyber Security Strategy and the UK law enforcement response.

21. In addition, the Crown Prosecution Service has a network of Criminal Justice Advisors and Liaison Magistrates posted overseas, who work closely with the British Embassy or Consulate and SOCA / the National Crime Agency. Criminal Justice Advisors are able to advise on cyber crime problems and initiatives, including proposals for reforms of laws and legal processes. The Liaison Magistrate network is more operationally focused, dealing with bilateral mutual legal assistance and extradition work. The Liaison Magistrate in Washington has particular expertise in advising on appropriate legal procedures required to obtain evidence from Internet Service Providers.

HAC 21. To this end, we cannot understand why the UK has refused to support funding for the new Europol Cyber Crime Centre EC3 which facilitates vital cross-Europe information sharing. E-crime does not recognise country borders and it is essential that we have strong international cooperation to ensure offenders are brought to justice and citizens protected. Strengthening our defences and international investigation capacity will save money in the long term and we recommend that the UK supports additional EU funding for the Centre. (Paragraph 73)

22. The Government does not accept HAC recommendation 21. The UK has welcomed the creation of the European Cyber Crime Centre (EC3) and is keen to see it encourage cross-EU working on cyber crime. However, Europol should fund the centre from within its existing budget, given the constraints of national budgets as a whole. The UK will work with the Centre and where possible, help shape it to support the work of Member States and engage with internationally. We are keen to see the EC3 develop to provide practical support to Member States on cyber crime, and to support the wider EU programme on capacity building, as outlined in the EU Cyber Strategy.

HAC 22. We are deeply concerned that EU partner countries are not doing enough to prevent cyber attacks from criminals within their countries on the UK. We will return to this matter in our inquiry into the proposal to opt out of the EU police and criminal justice measures which were adopted before the Treaty of Lisbon entered into force. (Paragraph 74)

23. The Government notes HAC conclusion 22 and the intention to return to this matter in a future HAC inquiry.

Cyber crime prevention:

HAC 3. It is of great concern that the majority of cyber crime could be prevented by better awareness by the user. Whilst the sophisticated threats will remain, we must do more to protect our information online. The Government and the private sector both have a strong incentive to educate users and maintain awareness of cyber crime. We recommend that, through its various channels, all organisations, businesses and schools must provide users with appropriate information and risk management training. (Paragraph 22)

24. The Government accepts HAC recommendation 3. In September 2012, the Government launched "Ten Steps to Cyber Security", a document focused at FTSE 100 companies, which details how to adopt simple measures to enhance cyber security[1]. In April 2013, the Government published a version for small businesses: "Small businesses: What you need to know about cyber security"[2]. The Centre for the Protection of National Infrastructure (CPNI) has also expanded its capacity to deliver targeted cyber security advice to senior audiences in companies that may be at risk from cyber attack. The Cyber Governance Health Check is a Government initiative which, with the support of the audit community, will help boards of the FTSE350 understand their threat and identify areas of vulnerability.

25. Businesses need to work to protect their customers. Government is therefore working with various sectors to consider how they can support this. This includes current work with Internet Service Providers to set out their agreed security offering to their customers.

26. To further educate the public and businesses on the risks that they might be vulnerable to, the Government will be launching a new national campaign in the coming months to help people and businesses understand how they can stay safe online. This programme will be delivered in partnership with the private sector and aims to increase cyber confidence and measurably improve the online safety behaviours of consumers and SMEs. It will build on work already done to raise awareness through initiatives such as Get Safe Online.

27. To assist the public to stay safe when using Government sites, an advisory tool has been rolled out across the .GOV.UK website and sections of the HM

[1] https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility.
[2] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/197177/bis-13-780-small-business-cyber-security-guidance.pdf

Revenue and Customs website which advises users if their internet browsers are out-of-date. Users can link to straightforward advice on what threat this might pose to their online security and how they can update their browser. This initiative is being carried out in conjunction with Get Safe Online, from where people can obtain further advice and information on how to stay safe online.

Data security:

HAC 26. Online services should be 'secure by design' e.g. new account settings should be set by default to private with the user sharing information with friends or publicly only if they actively choose to do so. Users should not be asked to submit personal details that are known to be helpful to fraudsters. For example, users should be discouraged from giving their date of birth. (Paragraph 101)

28. The Government supports HAC conclusion 26 and is working with companies to encourage them to consider the vulnerability of their products to criminal exploitation before being released to the public (see response to HAC recommendation 11).

HAC 32. We recommend that software for key infrastructure be provably secure, by using mathematical approaches to writing code. (Paragraph 112)

29. The Government supports HAC recommendation 32. To this end the Government has invested in the Trustworthy Software initiative, a public/private partnership initiative to develop guidance and information on secure and trustworthy software development. More information on this initiative is available at http://uk-tsi.org.uk.

HAC 27. We recommend that providers of web services take users through a short explanation when they sign up for an account about how to keep their data secure and how criminals could use certain data against them. Users should not be asked to provide such valuable personal data. (Paragraph 102)

HAC 33. We recommend that guidance about keeping personal data secure should be incorporated into all online services that request personal data from their users. (Paragraph 119)

30. The Government notes HAC recommendations 27 and 33 and is committed to working with industry partners to provide more information to users about how to act securely online. The National Fraud Authority has been working with private sector partners and others to educate users about online safety. This has been a core part of the 'Devil's in your Details' campaign, run by the National Fraud Authority and a key message of Get Safe Online activities.

HAC 28. We are concerned that many users may not grasp the full extent of the data they are sharing with private companies. The interest in and opposition to plans to increase data availability to the Government (e.g. witness the fate of the proposed Data Communication Bill) makes us question whether the public are really relaxed about sharing so much data or if they are simply unaware they are doing so. (Paragraph 103)

31. The Government notes HAC conclusion 28.The Government acknowledges that the use of personal data is an important issue for the public and is committed to being transparent in this area. This is why draft communications data proposals were subjected to a thorough pre-legislative scrutiny process by a Joint Committee of both Houses of Parliament. The Committee concluded there is a need for some further communications data to be retained, subject to appropriate safeguards, in order to ensure that law enforcement agencies can protect the public. The Government has made it clear that it will bring forward proposals, which may involve legislation, to tackle the problem of matching internet protocol addresses so that cyberspace cannot become a haven for criminality. These proposals will not allow the indiscriminate monitoring of the internet activity of members of the public. Our approach will be proportionate with robust safeguards in place.

<u>The cost of cyber crime:</u>

HAC 9. We understand that any measure of crime will always be subject to challenge and e-crime even more so. However we are puzzled that the Government continues to use highly controversial figures, in which independent experts or indeed other government departments such as the Ministry of Defence have little confidence, as its basis for policy-making. (Paragraph 38)

HAC 10. Improving the way in which e-crime is reported and recorded is key to improving Parliament's and the public's understanding of it. It is important that policy makers have an up to date and accurate estimate of the threats from e-crime. We therefore recommend that the Government publicly distances itself from the £27bn estimate of the annual cost of e-crime to the UK economy. (Paragraph 39)

HAC 11. We recommend that the Government commission a working group of experts, drawing on existing good practice already developed by academia and industry, to produce annual figures which show the incidence of e-crime and any observable trends. This group should include representatives from the cyber security industry and independent experts to ensure the figures are robust. (Paragraph 40)

32. The Government recognises the concerns set out by the Committee in conclusion 9 and recommendation 10. As the UK Cyber Security Strategy noted, “a truly robust estimate will probably never be established, but it is clear the costs are high and rising”. Based on the research available, it is reasonable to suggest that costs of cyber crime equate to several billion pounds per year. However to develop a more precise assessment of the cost of cyber crime, data on the prevalence of different types of cyber crime must be improved and expanded. This where the Home Office has been putting most effort, through its survey work, the setting up of Action Fraud and planned enhancements to crime recording.

33. The Government accepts recommendation 11. The Government will set up an external working group which would focus on providing improved estimates for the cost of cyber crime. This group will be led by the Home Office and comprise key academic and research partners. The group would seek to agree on the best available data, develop an agreed model for assessing costs and improve these estimates over time.

Cyber crime sentences:

HAC 15. We also note DCS McMurdie’s comments that e-crime sentences are too lenient. We were surprised by the fact Anonymous hackers who cost Paypal over £3.5m were given sentences of 7 and 18 months and do not believe they would have received such sentences had they physically robbed a bank of £3.5 million. The DPP should review the sentencing guidance and ensure e-criminals receive the same sentences as if they had stolen that amount of money or data offline. (Paragraph 56)

34. The Government rejects HAC recommendation 15. It is important that cyber criminals receive sentences in line with the severity of their crimes. Under the Computer Misuse Act 1990, offenders can receive up to ten years in prison for certain offences and a fine.

35. Sentencing guidelines are a matter for the independent Sentencing Council. The Sentencing Council is made up of judges and senior officers from criminal justice agencies, and gives courts guidance in assessing the seriousness of an offence. Courts are required by law to follow these guidelines when sentencing (although they can depart from them in exceptional circumstances if it is in the interest of justice to do so). The Guidelines assist in ensuring there is a consistent approach to sentencing, and the Council gives priority to offences which before the courts in highest numbers.

36. The Crown Prosecution Service has taken action to ensure that prosecutors have the skills and knowledge required to effectively conduct cybercrime prosecutions and present digital evidence in court, including through specialist cyber crime training.

Balance of National Cyber Security Programme investment:

HAC 6. Ministers have acknowledged the increasing threat of e-crime but it is clear that sufficient funding and resources have not been allocated to the law enforcement responsible for tackling it. Professor Ross Anderson told us that "we should be putting more of the cyber budget into policing and less of it into the intelligence sphere, into cyber war." We also note as a principle, that if personal data is held in any database, no matter how secure, there is a risk of it being accessed inappropriately, either through human error or malice. The only way to ensure data does not leak is not to collect it. (Paragraph 25)

37. The Government does not accept HAC conclusion 6. The Government has committed £860 million, over five years, through the National Cyber Security Programme to tackle the range of threats set out in the National Cyber Security Strategy. Cyber crime is one of these threats. More than 10% of the National Cyber Security Programme in 2013/14 is being invested in tackling cyber crime and developing new law enforcement capabilities, in addition to existing police funding.

38. A significant proportion of the National Cyber Security Programme funding is spent on GCHQ capability, and across the Security Intelligence Agencies so we can better understand the threat to the UK, improve our ability to detect attacks, and develop and sustain world class cyber capabilities and give the UK a competitive edge in the global cyber security sector. This investment is vital and underpins everything else the Government does on cyber.

Industrial espionage:

HAC 7. We note the increasing threat posed by state industrial espionage, and international e-crime committed for political purposes, such as the purported attacks on the Guardian from Syria and attacks from China on the US media. The Government must not underestimate the danger such attacks pose to our infrastructure and take firm action with offending countries to cease their activities, using international forums to raise these issues. (Paragraph 30)

39. The Government accepts HAC conclusion 7. The Government takes seriously threats of espionage and is working with companies that own and manage the Critical National Infrastructure (CNI) to ensure key data and systems continue to be safe and resilient - a commitment set out in the National Cyber Security Strategy. The Centre for the Protection of National Infrastructure is supporting

the UK's CNI and other priority companies to reduce vulnerability of cyber attack through the delivery of intelligence-led protective security advice. The Government regularly issues alerts, warnings and advice on mitigating cyber threats to organisations in the CNI and wider industry through the network of Computer Emergency Response Teams (CERTs).

40. Working with international partners is essential to enhance and support operational investigations and to develop norms of behaviour to make the internet a safer place globally. The UK is a leader in this space, setting up the first Cyber Conference in London (2011) and worked closely with the South Koreans to deliver the third conference in Seoul in October 2013. At the UN Group of Government Experts on Developments in the Field of Information and Telecommunications (UNGGE), the UK was instrumental in getting the group to agree that international law applies to cyber space and gaining momentum for the development of norms of behaviour and confidence building measures.

HAC 8. We recommend the establishment of a dedicated espionage response team that British companies, media, and institutions can immediately contact to report an attack and who can also provide training in order to counter attacks. (Paragraph 31)

41. The Government accepts HAC recommendation 8. It is important to ensure a robust, rapid UK response to any incidents of cyber espionage and other threats. That is why the Government announced in November 2012 that it would establish a new national Computer Emergency Response Team (CERT-UK) to improve national co-ordination of cyber incidents and act as a focus point for international sharing of technical information in relation to cyber security incidents.

42. This will build on existing dedicated channels for responding to threats of espionage and through which Government regularly issues alerts, warnings and advice on cyber threats. CERT-UK will bring different strands of the cyber response together to ensure an agile response to cyber threats. Internationally, a national CERT is rapidly becoming the accepted channel for engaging other countries on technical cyber issues. Moving in this direction will also simplify our engagement with other countries.

43. The Cyber Security Information Sharing Partnership (CISP), which was launched in March 2013, provides companies with a secure forum in which to exchange information on cyber threats and best practice with the Government and each other in real time.

Illegal content online:

HAC 29. We are deeply concerned that it is still too easy for people to access inappropriate online content, particularly indecent images of children, terrorism incitement and sites informing people how to commit online crime. There is no excuse for complacency. We urge those responsible to take stronger action to remove such content. We reiterate our recommendation that the Government should draw up a mandatory code of conduct with internet companies to remove material which breaches acceptable behavioural standards. (Paragraph 104)

44. Internet Service Providers (ISPs) are able to claim the hosting defence under the Electronic Commerce (EC Directive) Regulations 2002 only if they remove illegal content from websites that they host if they are notified of the illegality (the "notice and takedown" process). As an example of the effectiveness of this, the Internet Watch Foundation (IWF) Annual Report (2012) stated that when they issue notices for the removal of illegal content hosted in the UK, 56% of the webpages are removed within one hour. IWF Members remove 90% of such content within one hour, and 100% within two hours.

45. Where images cannot be taken down (for example if they are hosted in foreign jurisdictions) the IWF works with ISPs to block images of child sexual abuse. The result is that child abuse imagery is blocked on about 98.6% of consumer broadband lines in the UK. The Government urges all ISPs and hosting providers to join the IWF, and to improve their take down times. The Government therefore does not, at this time, support the Committee's recommendation for a mandatory code of conduct for the removal of material that breaches acceptable behavioural standards but will continue to keep this matter under consideration.

46. The Prime Minister's speech of 22 July outlined the wider steps that the Government is doing to keep children safe online – including steps to make it more difficult for paedophiles to search online for child abuse images. The Prime Minister was clear that the search engines need to do more in this area, to prevent results being returned when someone types in a term that is identified by CEOP as being used to look for indecent images, and that if the search engines do not make sufficient progress then we will look at legislative options.

HAC 30. We note those companies that donate to the Internet Watch Foundation, and encourage them to increase their contributions. Additionally, we recommend that the Government should look at setting up a similar organisation focused on reporting and removing online terrorist content. (Paragraph 105)

47. The Government supports the Committee's encouragement to industry to continue to financially support the Internet Watch Foundation (IWF).

48. The Government is considering HAC recommendation 30, and other actions to tackle online radicalisation, through the Prime Minister's Extremism Task Force. Where online content breaches terrorism legislation, a dedicated police unit is able to take swift action to assess and take down illegal web content. To date, the Counter Terrorism Internet Referral Unit (CTIRU) has removed over 6,500 pieces of material. Where material is hosted overseas, the priority has been to filter illegal web content (over 1,000 URLs) from the public estate.

49. CTIRU proactively seeks to identify illegal material. Members of the public who are concerned about extremist content online are able to refer material for investigation and take down by the CTIRU. In this respect, the CTIRU acts like the IWF in reporting and removing terrorist content. The Government is currently considering what can be learned from the IWF model. This work will report directly into the Prime Minister's Extremism Task Force.

Child safety online:

HAC 34. It is as important that children learn about staying safe online as it is that they learn about crossing the road safely. We welcome teaching about online safety and security taking place in schools and initiatives such as 'safer internet week'. (Paragraph 120)

HAC 35. The children we spoke to believed an important part of learning to stay safe online was being taught to respect others online and not to say things that you wouldn't say to their face and we agree. (Paragraph 121)

50. The Government acknowledges HAC conclusions 34 and 35. Online safety for children is of paramount importance to Government, and there are major cross-Government efforts taking place to ensure that children learn about staying safe online both in schools and through other initiatives. For example, as part of Government reforms to the national curriculum, we will be strengthening the requirements to teach e-safety as part of changes to the new computing programmes of study.

51. CEOP's work to educate children and young people focuses particularly on the implications of their online behaviour, the "digital footprint" they leave, and the range of contact, content and conduct risks they face online. CEOP has developed a specific educational programme called ThinkuKnow to tackle this issue. The programme includes educational films and cartoons, teachers' packs and other online resources for use with children aged 4-18. In 2012/13, over 2.6 million children saw the ThinkuKnow resources. In the same year, over 800 professionals in education, child protection and law enforcement weretrained by CEOP to educate children about online safety and how to respond to incidents. The Government, through CEOP, has now trained over 25,000 professionals who deliver these key messages to children in classrooms and other youth settings.

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

The Houses of Parliament Shop
12 Bridge Street, Parliament Square
London SW1A 2JX
Telephone orders: 020 7219 3890/General enquiries: 020 7219 3890
Fax orders: 020 7219 3866
Email: shop@parliament.uk
Internet: http://www.shop.parliament.uk

TSO@Blackwell and other accredited agents

ISBN 978-0-10-187342-0