

Chapter 7

Digital Security and Safety

"We have always had the ability to create structures that are quite bewildering to us. A good example is a city. I would say that the Internet is more like a city than anything else. In cities there are slums, there are palaces of wisdom, libraries, museums, art galleries, theatres, places of entertainment and shops. And there are places in those cities where you would not want to go down dark alleys let alone have your children do so, but slowly we let our children learn to use the cities and they do."

Stephen Fry – Digital Britain Summit

AMBITION: TO ENSURE THAT EVERYONE CAN LIVE AND WORK ONLINE WITH CONFIDENCE AND SAFETY

INTRODUCTION

1. As the move from analogue to digital is radically changing our network infrastructure, our creative industries, the delivery of Government services and many other areas highlighted in this report, so it will require our policy, regulatory and legal frameworks around security and safety to adapt to the transition to digital, global networks.
2. Most of the risks of the real world – short of direct physical harm – are replicated in the online world. Potentially harmful and offensive material can be created and disseminated, lies can be told, scams perpetrated, privacy invaded, vulnerable people led to harm themselves or others. And there is the risk of attacks to the system itself and individual parts of it which are critical to governments, businesses and individuals.
3. What is illegal offline is also illegal online. But whilst online the criminal is digital, the protector and enforcer is often still analogue: certainly our frameworks for online protection have not kept pace with 200 years' development of consumer protection law and enforcement in the offline world. The Government recognises that, as a society, we need to catch up.



4. It is not the Government's policy to react to the challenge of the change the Internet presents by retreating to a position of protectionism or oppressive regulation. But questions around online security, Internet governance, regulation and consumer protection will be brought into much sharper focus as we move toward a ubiquity of broadband where more and more of us are digitally domiciled.
5. Whilst ultimately, the Internet cannot be made risk-free if it is to function effectively, governments, businesses, civil society and individual users can and must share responsibility for minimising the risks. And due to its global nature, issues relating to governance of the Internet are often outside the jurisdiction of individual national governments and regulators. Responsibility for ensuring that Internet governance is effective therefore needs to be considered at three levels:
 - at the global level, recognising the cross jurisdictional nature of today's networks;
 - at the national level, on those issues where appropriate national action remains a highly effective tool; and
 - at the consumer level, through appropriate action and by empowering all of us to take steps to protect themselves.
6. The rest of this chapter considers each of these three areas.

GLOBALISATION AND THE INTERNET

7. The Internet is the first truly global network, connecting nearly a third of humankind – now approaching 2 billion users – worldwide. It crosses international boundaries allowing instant global communication, sharing and dissemination of information across multiple international jurisdictions at the click of a button. Cyberspace does not have national borders.
8. Many of the companies that have evolved with the Internet are today instantly recognisable global brands. Companies such as Google, Yahoo, eBay and others have used the global scale of the Internet to reach millions of customers in timescales that were previously unimaginable. In 1999 Google employed 8 people. This year it became the world's first \$100bn global brand.
9. The Internet is in essence a participative, generative network promoting interactivity, collaboration and conversation. It is a place where people can share and shape information, upload their own content and edit and recast other people's creations, inviting all of us to become innovators, editors and creators. And we communicate, transact and share globally across the Internet. It is one of its greatest strengths.
10. It is also a fundamentally different network to its analogue predecessors, which were confined within national borders and subject to clear national jurisdiction. In considering questions around digital security, no free, democratically-ruled, country can afford to make the mistake of starting from our current systems



and considering how we can adapt them to the online environment. Rather, we must evolve new models and approaches that are in harmony with the global nature of the Internet.

11. Other countries with very different political systems may seek to adopt different approaches, based on keeping analogue systems of control in the digital age. The Government believes this to be both undesirable and unsustainable.
12. In a global economy we must respect the particular approaches that different countries adopt. We cannot assume that only one global model fits all sizes. But we should take the Internet pioneers' assumptions of freedom, entrepreneurialism and untrammelled innovation as the base model. Particular national approaches should be respected as the exception rather than as the rule. If some countries still seek to deny the global nature of the Internet, they must accept the consequences in slower access to information and growth. They cannot assume a veto on the Internet's worldwide growth or on its global governance.
13. One means of achieving this global coordination is firstly through the Internet Governance Forum (IGF), which provides an international platform for sharing information and best practice, addressing issues such as the global digital divide and increasing access to the Internet worldwide, trust, safety and the impact of future technologies. The IGF has, since 2005, provided a crucial platform for information sharing and dialogue on topics critical to global, social and political development, fostering the sustainability, robustness, security, stability and development of the Internet.
14. Some governments have criticised the IGF for not being able to take decisions. We in the UK believe however that this is in fact one of its fundamental strengths. Without being subject to the constraints of an international negotiating forum, the IGF is able to bring together all the key stakeholder experts from across the globe to identify the best policy approaches, the available technical solutions and the way forward for innovators at the edge of the Internet to have a real immediate impact.
15. In addition to the yearly sessions of the IGF, vital work undertaken by the Internet industry and its communities happens all year round. The UK was one of the first countries in 2007 to develop this multi-stakeholder model at the national level. Sponsored by the ".uk" registry Nominet with support from BIS and a Parliamentarian group led by Alun Michael, MP, the aim of the UK IGF is to prepare UK inputs in the run up to the global annual IGF and subsequently to disseminate its outputs to the wider UK Internet community while generally maximising UK stakeholder engagement in the IGF process. The UK IGF has become a role model for other national and regional IGFs which have emerged worldwide in the last 12 months.
16. The IGF today is at a crucial turning point. The IGF was set up for an initial period of five years. Discussions are now taking place about whether the IGF mandate should be renewed, and if so whether it should be changed in any



way, with the possible extension of the IGF beyond 2010. The final decision on the future of the IGF will be taken by the UN General Assembly in late 2010. **The UK Government supports the continuation of the IGF for a further five year term continuing to represent all stakeholders involved. The UK does not support any move towards the IGF transforming into a new UN Agency or being subsumed within an existing one.**

17. The second key multi-stakeholder forum with a crucial role in ensuring that the critical infrastructure of the Internet remains robust, resilient and supportive of innovation and growth, is the Internet Corporation for Assigned Names and Numbers (ICANN). ICANN provides a coordination role of the Internet's domain naming system. It is a not-for-profit private sector organisation based in California. There are countries that see ICANN's operational role with regard in particular to country code domain names and the introduction of non-Latin based scripts such as Arabic and Chinese as impacting on their national sovereignty over critical Internet resources.
18. The future role of ICANN's Governmental Advisory Committee (GAC) will be crucial in ensuring that ICANN's management take full account of the views of all governments on DNS issues that concern public policy. The UK will continue to contribute to the GAC's work in making recommendations that ICANN will adopt in its policy-making process, and to ensure that ICANN remains resilient, robust, immune to capture by any specific interests, and fully accountable to the global Internet community. **The UK strongly supports ICANN continuing as the unique not-for-profit multi-stakeholder organisation with responsibility for the management of the domain name system and it taking a leadership role in improving standards of the security in the key protocols, processes and technology that underpins the use of the domain name system.**

How Do Domain Names Work?

The domain name system (DNS) is the addressing system for the Internet and is used to give each host or computer on the Internet a unique name (e.g.. www.culture.gov.uk). There are two sorts of domain names: either Generic Top Level Domains (gTLDs) , such as .com, .org, or Country Code Top Level Domain (ccTLDs) such as .uk and .fr. Computers or hosts are identified by their IP number, a string of digits analogous to a phone number. 89.234.33.13 is the IP number for www.culture.gov.uk. It is the IP number which is used to route Internet traffic around the world, not the domain name. At the top of the DNS management structure is ICANN. ICANN co-ordinates these unique IP numbers around the world and decides which organisations can operate a particular Top Level Domain. The central register of .uk domain names is managed by Nominet, a not-for-profit company. Nominet is an active member of the ICANN ccTLD community.



19. In 2008, ICANN proposed the introduction of a new policy that would allow applications for an unlimited number of generic Top Level Domains (gTLDs). These would potentially include not only purely generic names like .sport but also geographical ones like .france and brand names like .nissan. If the current policy approval process runs its course and implementation of the application procedure is successfully put in place in 2010, ICANN's assessment is that it expects to receive approximately 500 applications from potential registries to run new gTLDs of which perhaps 200 may prove successful. Some of these new registries may well be based in the UK and this is expected to have a significant impact in promoting greater competition in the domain names market and in enhancing participation in the development of the global Internet.
20. The domain system is a crucial element in the Internet economy. Without a smooth running system, including a well functioning registration process, the Internet as we know it might grind to a halt with the knock on effects to the wider economy. The .uk domain system itself is an important asset for the UK. Nominet operates at the heart of e-commerce in the UK, running one of the world's largest Internet registries and managing over seven million domain names. It is highly respected within the domain name community including internationally.

Nominet's Corporate Governance Review

To address concerns expressed by the government about how Nominet's constitution and structure met its stakeholder responsibilities, Nominet commissioned an independent corporate governance review conducted by Professor Bob Garratt. The recommendations of that review were published in April 2009. They included creating a separate role of Managing Director; revise the system of voting for directors; appointment of non-executive directors; broaden the membership; revision of the voting arrangements to achieve a fair balance across the membership. The Government has welcomed the Review's recommendations which we hope will be implemented. We look forward to the response of Nominet's membership.

21. For years the .uk domain name industry has been self regulated without need for Government intervention and this has largely worked well. Nominet has ensured at the same time that all wider stakeholder interests are taken into account. There have however been reported abuses of the domain name system such as cyber-squatting, drop catching, pressure sales of domain names and poor registration practices. If the successful self-regulation were to fail through a failure to address the concerns identified in the Nominet governance review, then the Government would have to intervene in order to protect consumer interests and guarantee Internet users in the UK that the domain name system will remain coherent and continue to function in their interest.



22. In view of this, the Government has decided that on a precautionary basis it will seek reserve powers in any appropriate forthcoming legislation to regulate against the risk that the entry into the sector of a number of new, and as yet unidentified, players will mean we need a basis for industry cooperation. These powers may, for example, enable the Government to direct Ofcom to regulate the distribution of domain names in the UK, possibly by setting conditions and establishing a code of practice to which the industry would be required to conform.

THE NATIONAL APPROACH TO DIGITAL SECURITY

23. Whilst global collaboration will be increasingly important, there remains a significant and critical role for appropriate action at the National level to help shape a safer online world.
24. Ensuring that the UK has a world class approach to digital security will bring significant benefits:
- UK networks will be seen as safe and reputable (where perhaps others are unreliable or more vulnerable to criminal exploitation).
 - The intellectual property of businesses, universities and other institutions, which underpins a knowledge economy, will be better protected.
 - Businesses using UK networks will gain a competitive edge in the global marketplace.
 - UK citizens and business will prosper as the volume of business transacted securely online continues to increase.
 - UK citizens will have greater confidence in public service transactions; thus yielding efficiencies and cost saving.
 - And the businesses that have delivered secure functionality will have opportunities to sell their services globally on the back of UK success.
25. Any steps taken by Government must balance the needs and rights of the user, the reality of what is possible and the needs of business, delivering a proportionate policy and regulatory approach.
26. The rest of this Chapter considers the specific steps required at a National level to meet these ambitions, under three distinct headings:
- **High Level Cyber Security:** by which we mean the approach to high level network security and to serious and organised crime and terrorism, often taking place at a supra-national level;
 - **Personal Digital and Data Security:** by which we mean the approach to making consumers safer online in relation to online scams and rip-offs, identity and data privacy and personal network protection; and



- **Content Safeguards:** by which we mean protecting consumers from illegal content and protection of certain vulnerable groups from potentially harmful material, particularly children.

HIGH LEVEL CYBER SECURITY

27. If we are to be successful in meeting the complex and inter-dependent challenges of Cyber Security, it will be vital to work with all sectors in the UK, as well as international partners. E-crimes relating to illegal access, illegal interception, data interference, botnets and other issues often require today cross-jurisdictional cooperation.
28. The UK's National Security Strategy describes how 'cyber security' cuts across almost all the national security challenges that it identifies, and the need to address them in a coherent way. To this end, the Government is developing a Cyber Security Strategy to build a safe, secure and resilient cyber space for the UK, through both the beneficial exploitation of cyber space and the reduction of risks posed by those who seek to do the UK harm: the forthcoming Cyber Security Strategy will set out how the Government intends to approach this task.
29. It is important that our networks are resilient, that is that they can withstand and recover from deliberate attack and the impacts of problems such as severe weather. In the UK, the emergency plan for the communications sector is owned by the industry and the Government and industry work together to ensure that the industry emergency planning reflects the latest understanding of the nature of the threat and that lessons are learnt from events that have led to network problems (e.g. the 7/7 attacks in London). These arrangements hinge on rapid and effective communication between the companies in emergency situations and communications with the Government to allow the right level of central Government involvement in the management of the emergency on the ground. These communications arrangements are regularly tested and reviewed. **The Government will carry out a major test in late 2009 of our ability to manage and recover from a major loss of network capacity.**
30. It is important that there is a greater appreciation of the work undertaken to keep our networks running and allow a broader stakeholder input into that work. **For that reason we have asked the chairman of the Electronic Communications Resilience and Response Group (EC-RRG) to make publicly available the planned report to the Secretary of State for Business, Innovation and Skills on the work of the group in the past year and going forward.** We also welcome the intention of the group to hold a workshop to involve stakeholders in the direction of the Group.
31. Some elements of our infrastructure can be regarded as critical in terms of the nation's ability to carry out essential functions. The Government recognises that special attention needs to be paid to this infrastructure. Accordingly, the Centre for the Protection of National Infrastructure (CPNI) works with BIS to



identify key threats to critical communications infrastructure, and the Government works with the key companies to address any vulnerabilities that may exist. CPNI have also created a forum for industry experts to identify emerging problems and solutions.

32. A key question is how security can be assured at those points where one provider's network interconnects with others. An industry agreed voluntary adoption of minimum security standards will be the first step in preparing the UK for the forthcoming increased legal requirement on security standards that is likely to be introduced following the agreement of a new European Framework for the regulation of communications networks and services.
33. The work that has been undertaken in the UK in relation to Critical Infrastructure Protection and the resilience of communications networks has been one of the key models for the development of European policy thought in this area. In March this year, the Commission published a Communication on Critical Information Infrastructure Protection – "Protecting Europe from large scale cyber attacks and disruptions: enhancing preparedness, security and resilience" – which proposed activities that could be led by the Commission over the next two years. One of the drivers for this work was the attack on key web sites and Internet infrastructure in Estonia in 2007. It was fitting therefore that the Communication was discussed in a Ministerial Conference held in Tallinn, the capital of Estonia, in April 2009. This conference broadly welcomed the focus of the Communication on how efforts may be best directed to ensure that Europe improves its performance in understanding risk, taking appropriate resilience measures and testing those measures in exercises.
34. The UK will play a full part in the work arising from this Communication and also welcomes the opportunity to contribute to the broader issues around the direction of Network and Information Security policy in Europe that is expected to culminate in a Commission Communication in 2010. With our relative strengths in these areas, we are well placed to influence thinking in this area and to test the continued relevance of our policies against the wider European experience. One aspect of the discussion will be to look again at the role the European Network and Information Security Agency may play in delivering an economically stronger Digital Europe.
35. The Government also recognises that e-crimes, whilst not always of themselves different to offline criminal activity, do require particular skills to investigate them, which requires providing the necessary support for law enforcement. The National Hi Tech Computer Crime Unit was established as a specialist e-crime unit and was folded into the Serious and Organised Crime Agency in 2006. The Government recently announced the establishment of a specialist e-crime unit, the Police Central e-crime Unit (PCeU), based in the Metropolitan Police, and we will be establishing a National Fraud Reporting Centre. The Government supports the SOCA e-crime unit, which tackles cybercrime internationally. But a vast amount of e-crime is small scale and aimed at home users through the use of malicious software and deception. This is addressed in the next section.



36. We welcome proposals brought forward to us by Alun Michael MP, chair of the the Eurim e-Crime Group, to enhance the levels of coordination between different groups and initiatives across the e-crime spectrum. We believe that there is significant value in achieving this ambition. **We will therefore explore the formation of a new tripartite initiative, the Tripartite Internet Crime and Security Initiative, between parliamentarians, Government and business to look across the spectrum of issues and responsibilities and at a practical level look at promoting new efforts in the self regulatory sphere. This initiative, chaired by Alun Michael MP, will complement the work of SOCA, e-crime, the Police Central e-Crime Unit and the National Fraud Strategic Authority.**

PERSONAL DIGITAL AND DATA SECURITY

37. Consumers must be able to communicate, trade, order services and work online with confidence. The networks and services they use must be available and reliable. Their private data (e.g. bank details) must be secure from misuse or fraud. Consumers must have confidence and be able to check that people they are trading with or working with online are who they say they are and can be trusted.
38. Getting to this level of confidence requires users to know enough about the dangers from hackers, viruses and fraudsters to take basic steps to protect their own data. Service providers must react quickly to instances of fraud and to patch vulnerabilities that are discovered. And suppliers must make their products more secure against digital threats. We will not succeed in our goals if consumers turn away from the online world through fear that they will be robbed or that their personal information will be exploited.
39. Giving users basic advice about avoiding known problems online must be a cornerstone of any approach to improving security. To that end, the Government has worked with the private sector to create GetSafeOnline which offers advice in plain English on protecting your PC, avoiding online rip offs and taking care of your identity online. The GSOL initiative has reached maturity in terms of its ability to produce the right material for its audience, but lacks resources to deliver a greater impact.

Get Safe Online

Get Safe Online was launched in November 2005 as a major public-private sector initiative to raise awareness of online security. Get Safe Online is sponsored by the Government, Serious Organised Crime Agency (SOCA), Microsoft, HSBC, Cable & Wireless and Ofcom. It is aimed at consumers and micro-businesses. Government funding is provided by the Cabinet Office.



The Get Safe Online campaign is largely Internet based. The website (www.getsafeonline.org) is a one-stop-shop for reliable, up-to-date information about online safety, to give home users and small businesses the advice they need to use the Internet safely. It includes information on protecting your PC, yourself and your business as well as advice on topics such as Internet shopping, social networking sites (Facebook, MySpace), data theft and identity fraud.

The key messages of the campaign are that online sales and transactions are increasing at an incredible pace. Get Safe Online wants people to be able to continue using the Internet, enjoying the many benefits it has to offer, but also to be aware of the risks and take the steps necessary to protect themselves and their families online. In addition, people are increasingly opting to use the Internet when transacting or interacting with Government and it is important they are online safely and securely.

40. We believe that the GetSafeOnline campaign can provide a significant contribution to helping consumers to take steps to protect themselves, not least because the GetSafeOnline name and branding has significant potential and is easy for consumers to remember and therefore access. Government and the private sector will need to continue to work together to ensure that the potential of the GetSafeOnline initiative is maximised.

SECURING HOME NETWORKS

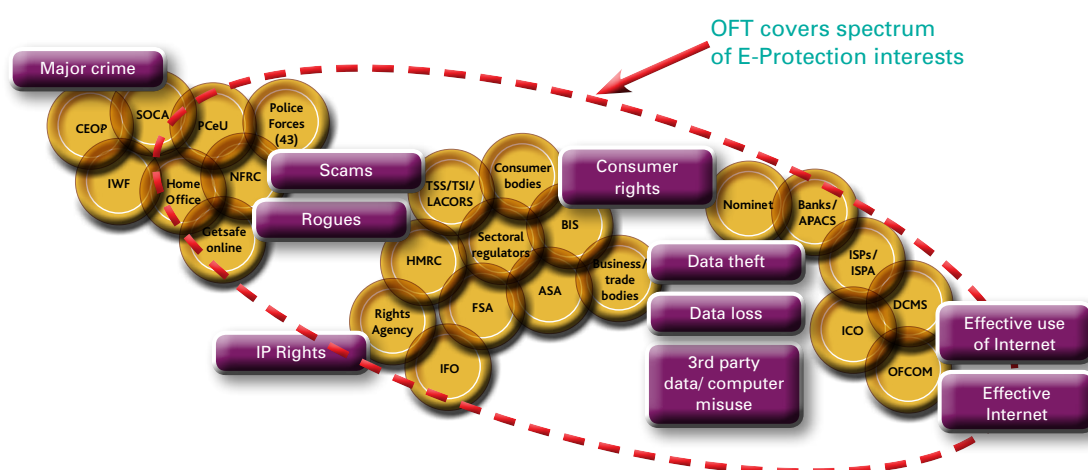
41. As home networks and technologies becomes more complex it might be thought that the challenges consumers face become even greater. However, this needs to be balanced against the reality that not only are consumers are becoming more able and used to technical products, but also technical products are becoming more user friendly in their design.
42. Providers such as Symantec and McAfee are today household names, providing easy to use and install security software at affordable prices both online and in physical form. These products make it easy for most people to take significant steps to protect themselves and their computers.
43. In addition, the market is increasingly providing a high level of after sales support to its customers through additional assistance in relation to dealing with technical complexity – a sort of “AA breakdown” assistance for your personal networking needs. As home networks become more complex, it is legitimate to expect that these types of service will continue to grow. Services such as “the Geek Squad” from Carphone Warehouse and “Tech Guys” at PC World provide consumers with fast and effective advice on a range of issues including computer optimisation, device set-up, software installation, parental control set-up and tuition, security and software installation, back-up services and many others.



ONLINE CONSUMER PROTECTION

44. Finally, the Government also recognises that existing mechanisms for consumer protection in the online world are complex and overlapping, with trading standards, the police, Ofcom and OFT all having a role. Good enforcement of consumer rights requires sufficient capacity to deal with the complex issues, effective joining up between agencies and the right interface with consumers. All of these are challenges that will require a fresh consumer strategy.
45. Online consumer protection is different because consumer behaviour is different online:
- Search costs may be different;
 - The cost and benefits of regulation may be different;
 - Consumer behavior may be different;
 - Consumer power may be different;
 - The balance of responsibilities in the transaction may need to change, or be reinforced; and
 - New forms of trading may pose new policy issues.
46. Added to this, the institutional structure for addressing the spectrum of consumer interests online is a very complex one. Today there are a large number of organisations wrestling with how best they can contribute to the challenge of protecting consumers online, including the police, the ICO, the OFT, Ofcom, the Home Office and others. The diagram below sets out the spectrum of organisations tackling e-protection issues in the UK today.

Figure 8: Institutions addressing consumer interests online



47. The OFT has made clear that to date it has not done as much as it would have liked to ensure that consumers can have confidence in the online medium and has put forward a five point plan, covering:
- Setting up a Consumer Direct front end with online reporting;
 - Acting as a clearing house for Trading Standards services;



- New enforcement activity;
- A new e-policy programme; and
- Campaign and consumer/business education activities.

48. The Government welcomes the OFT's offer to do more to play a full part in Digital Britain. Its knowledge and expertise from the offline world means that it can make a huge contribution in this area. If the OFT is to play a pivotal role, as it is equipped to do, it will require more clarity over its role, clarity over jurisdiction and the responsibilities of itself and other public sector bodies in this space and potentially additional funding.
49. **The forthcoming Consumer White Paper, to be published later this Summer, will outline how UK enforcers including the Office of Fair Trading, Trading Standards and the Police, as well as business, could work together on national issues regarding online fraud and other consumer protection crime in order to gather intelligence and tackle them effectively.**
50. A further growing area of concern for the Government is the disparity between the various penalties that Ofcom can impose under the Communications Act 2003 in relation to actions causing consumer harm. For example, where Ofcom has found breaches of the Broadcasting Code regarding phone-in scandals and the consumer harm they caused, it has been able to impose fines of well over £1m. Conversely, where Ofcom has found serious breaches of its rules on persistent misuse of a network or service, in particular in relation to extremely high numbers of silent calls (where the people receiving the calls had no method of knowing who had made them, with the resulting consumer harm), the statutory ceiling as currently set only allows Ofcom to fine up to £50,000. It seems to the Government that the discrepancy between these levels of fine is no longer sustainable or desirable. **The Government will therefore consult on the penalties that Ofcom is able to impose for contraventions of the Communications Act 2003 and, in particular, the level of the fine it can impose in relation to persistent misuse cases.**
51. Finally, one particular issue that has been raised with us is the funding of advertising self regulation. What has worked well in the offline world is the very small levy on all advertising collected by the advertising agencies on behalf of advertisers and paid to the ASA's Board of Finance. In the online world, this mainly holds true for banner advertising but this system appears not to be functioning so well for other forms of advertising, such as click through, as more and more advertisers place direct business with the aggregators, who to date have not adopted the vital collecting function of the agencies. The Government urges all parties to work together to resolve this because in the vital area of advertising consumer protection, online as well as offline, the alternative to effective self-regulation cannot be no regulation and often by default this becomes statutory regulation. This would not be the Government's first preference.



DATA SECURITY AND ASSURANCE

52. The issue of privacy and security of data online is a serious and growing one. A small number of high-profile cases have demonstrated the strong feelings that data privacy can provoke, and the complex relationship we have to the handling of different types of personal data and different types of consent.
53. It is an issue that is likely to become more and more important over the coming months. Research conducted by the Communications Consumer Panel earlier this year confirmed that this is an area of particular concern for consumers and new business models such as targeted advertising and new services such as Google's Streetview have taken this issue to front of the public's mind.
54. If handled properly, new business models such as targeted advertising could be important revenue earners because, as Meglena Kuneva, EU Consumer Affairs Commissioner said in March this year: *"Personal data is the new oil of the Internet and the new currency of the digital world."*
55. The ICO and the Information Commissioner have taken the initiative in addressing the principles which should apply to the use of personal data, building on the bare legal requirements of the Data Protection Act and focusing on ways in which businesses and individuals can mitigate risks from the provision and use of online data. Businesses that collect and use personal data for commercial purposes are required to respect user rights including access to personal data. Businesses are legally responsible to the ICO. **We support the ICO's plans to develop a new code of practice "Personal Information Online" for consultation later this year.**
56. The challenge is to demonstrate value to consumers while ensuring that there is no risk of abusing personal data, for example by developing mechanisms to ensure transparency, and at this stage the industry has yet to bridge that gap. The Internet Advertising Bureau (IAB), the trade association for online advertising in the UK, holds regular events that focus on a guide to behavioural advertising. The IAB also acts as a source of information about Internet advertising issues and promotes industry-wide good practice principles for providers who collect and use data (personal and anonymous) for behavioural advertising.
57. The IAB also covers user education, notice and choice broadly mirroring the Network Advertising Initiative (NAI) principles in the USA, but adapted to the EU data protection framework. **The Government welcomes the IAB's proposal to launch a consumer information portal about behavioural advertising.**
58. In developing a digitally engaged community in the UK, and allowing the development of new businesses to generate economic growth and innovation, the Government of course needs to uphold protection of privacy and the principle of transparency. This will always remain a guiding principle. But we also need to ensure that apparent concerns are properly assessed and understood, and that artificial barriers do not spring up.



59. In addition, Government must be increasingly vigilant in the manner in which it handles data. Government has already invested considerable resources into improving their data handling capabilities and will continue to treat this as an area of priority. We consider this issue further in Chapter 8.

ONLINE CONTENT SAFEGUARDS

60. For the reasons set out above and in the context of the new global digital world we have described throughout this Report, the Government to date has supported industry's desire to adopt a self regulatory approach in relation to online content safeguards. The Government acknowledges that industry has taken some important steps forward and that a number of self regulatory initiatives are taking place. The Government's preference remains for effective self regulation, but with the emphasis on effective.
61. **In order to maintain acceptable media standards and continue to build public trust and confidence in the self regulatory system through an evolving media landscape, it is of critical importance to ensure that self regulatory systems are properly resourced.**
62. There remains scope for further development of information and tools to help users manage their online experience safely and securely. There are already sophisticated tools to support parental controls and search preferences, dynamically updated using artificial intelligence. But users need to deploy them. More could be done to meet the public desire for information so that we can all decide for ourselves what content to access and how to protect ourselves better.
63. The rest of this Chapter considers two specific areas of concern and the ongoing work on those areas. Firstly, tackling criminal material on the Internet. Secondly, child safety on the Internet.

CRIMINAL MATERIAL ON THE INTERNET

64. The Internet Watch Foundation, based in Cambridge and with just 15 employees, is tasked with minimising the availability of criminal content – specifically, child sexual abuse content hosted anywhere in the world and criminally obscene and incitement to racial hatred content hosted in the UK. It works with law enforcement agencies worldwide and operates a "notice and take down" procedure in relation to content on UK sites and a list of international child abuse sites that ISPs can block at the network level. The vast majority of UK networks use this list and discussions are under way to ensure that relevant consumer networks are comprehensively covered.
65. As a result of the partnership approach adopted by the IWF, less than 1% of child sexual abuse content, known to the IWF, has been hosted in the UK since 2003, down from 18% in 1997. The IWF's work remains invaluable to every part of the value chain in the UK's Internet industry. And, in a world of universal



availability, increasing take-up and enhanced services on the network the work of the IWF will become more and more important.

66. IWF's current income includes a contribution from the EU Safer Internet Action Plan with the bulk being derived from voluntary membership subscriptions. Its current income equates to some £1m per annum. This voluntary structure means that there is no certainty that the level of funding received now from the EU or from its membership will continue at this level in the future. In the current economic climate a voluntary funding base carries with it increased uncertainty over funding. Whereas having secure funding would allow the IWF to consider expanding its internal skill base, especially with regard to hiring additional technical expertise and raising greater awareness amongst Internet users about their role and remit. The IWF model of self-regulation is a success and is admired internationally, but if the regulation of criminal content is not adequately funded by industry, Government would need to consider statutory intervention. **We therefore call on the IWF membership to propose a more secure funding model for the future.**
67. The IWF has also been a model for international hotlines for reporting child abuse material, especially across the EU. Some operators already use its list of illegal sites internationally. Since most child abuse material originates outside the EU, there is a case for its operations to cover at least the whole of the EU. **We will therefore explore with the IWF and the European Commission the scope for a pan-European model with commensurate funding.**

CHILD INTERNET SAFETY

68. Secondly, child safety on the Internet. The UK Council for Child Internet Safety (UKCCIS) was founded following the report by Professor Tanya Byron into the risks from exposure to potentially harmful or inappropriate material on the Internet and in video games. Chaired by DCSF and Home Office Ministers, the Council brings together more than 100 stakeholders from across the Internet safety spectrum who have come together to work in collaboration for the good of children and families. The Byron Review envisioned a strategy, led by UKCCIS, which would have two core elements:
- better regulation in the form, wherever possible, of voluntary codes of practice that industry can sign up to; and
 - better information and education where the role of Government, law enforcement, schools and children's services will be key.
69. Four Working Groups have been established to take forward work on industry standards, video games, public awareness and better education. Building on their work, UKCCIS is developing its long-term Strategy to improve children's safety. Work on children's Internet safety will have direct benefits for all users. For example the Social Networking Guidance developed by the Home Secretary's Task Force on Child Protection on the Internet which preceded UKCCIS, applies



to all social networking sites. It has now been developed and adopted at EU level, with a self-reporting mechanism to help monitor compliance.

70. The Government has set up the Child Exploitation and Online Protection Centre (CEOP) to help protect children online. CEOP runs the 'Think U Know' website, which is the main UK law enforcement website for providing children, young people and adults with information on how to keep themselves safe online.
71. One of the recommendations from the Byron review was to provide an authoritative "one-stop shop" for public information on child Internet safety. This is likely to include a website portal based at Directgov. There would be significant merit in further consideration of how this portal could be effectively linked to the GetSafeOnline portal and to information on how to protect personal data online, including linking to the ICO's consumer advice, to provide a comprehensive "one stop shop" for all aspects of online safety.
72. **If such a portal were created, the National Plan for Digital Participation should be used to support and promote the one stop shop for the provision of full information about getting safe online.**

CLASSIFICATION OF VIDEO GAMES

73. **Finally, the Government will adopt a new and strengthened system of classification for boxed video games incorporating the newly enhanced Pan European Game Information system (PEGI).**
74. A consultation was carried out between July and November 2008, which solicited comments about four potential options to amend the current system for classifying video games.
75. We have selected the Enhanced PEGI system, as it combines the best of a pan-European self regulatory system designed specifically for video games with a strong UK based statutory regulator taking account of the views of the UK public. It will give consumers a single set of clear logos for video games that will apply across most of Europe, providing an international solution for game content regulation. It has the flexibility required to adapt to the challenge of rapidly-evolving technology in the games sector and will be highly effective in the online world.
76. This system meets all the key criteria set out by Professor Tanya Byron in her report "Safer Children in a Digital World" and will offer improved protection for children including, for the first time, making it illegal to sell games suitable for 12 and older to underage children.
77. PEGI Online is also part of the range of online safeguards helping parents and children determine what content is appropriate, including BBFC.online and the new system for regulating television on-demand being established to implement the Audiovisual Media Services Directive.



FUTURE APPROACHES TO ONLINE CONTENT SAFEGUARDS

78. Industry, working with Government and others, has taken some significant steps in relation to self regulation of Internet-based services. In addition to the other examples in this Chapter, we would cite the following:
- 1) Ofcom, in partnership with the Home Office and industry, has worked on the development of a British Standards Institute (BSI) Standard for Internet content control software, which will help parents to make informed choices about the best filtering products to protect their children. The first Kitemarks based on the standard are due to be awarded in 2009;
 - 2) A self-regulatory initiative facilitated by the Broadband Stakeholders' Group which has created Audiovisual Content Information Good Practice Principles. These commit signatories to providing clear, consistent information about commercially-provided audiovisual content. Signatories include AOL, BBC, Bebo, BSkyB, BT, Channel 4, Five, Google, ITV, Microsoft, Mobile Broadband Group (represents Orange, O2, 3, T-Mobile, Vodafone and Virgin Mobile), MySpace, Teacher's TV, Tiscali, Virgin Media, Yahoo!, ATVOD (Association for Television On Demand), BBFC (British Board of Film Classification), FOSI (Family Online Safety Institute); and
 - 3) The Home Office Task Force Guidance on social networking, which produced an evidence-based set of standards for providers of social networking services, including u18 privacy settings, educational material and report abuse tools. This work formed the basis of EU level guidance published in February 2009 – a good example of where UK leadership in this field is now benefiting users in other EU markets.
79. As this Chapter makes clear, the Government continues to support further action and vigilance from industry through self-regulation in the first instance. We urge industry to continue to build on its good work to date to help consumers make appropriate and informed choices about the content they view on the Internet.
80. However, it is clear that there remains an important set of public policy questions to be asked about standards on the Internet and much legitimate debate to be had about how as a society we want to address those questions. Too often those questions are shrouded by unhelpful and loose phrases such as "Internet regulation", which provoke unhelpful and vitriolic responses.
81. The Government considers issues of Online Safety and Security to be of the utmost importance and a continuing and informed debate is needed to ensure that as a society we make the right choices in the future. As we move toward a world of ubiquitous broadband, governments around the world will need to be increasingly engaged and open about the right mix of approaches to these issues.



CASE STUDY

Older E-Users

John and Marianne Pritchard-Jones, both in their eighties, would not describe themselves as “silver surfers”. But the couple are wedded to technology, which they say enables them to keep track of family and enjoy TV shows at a time of their choosing.

The pensioners are already on their second generation of digital equipment, using a new computer, high-speed Internet connections, mobile phones and a digital radio – much of it acquired at the insistence of their children and grand-children.

For Marianne, who uses her birth year – 1927 – in her email password, the main benefits include receiving Flickr pictures from a grand-daughter touring New Zealand. She also goes online to access Welsh-language television, while using desktop publishing to produce a local history of war memorials.

“I would never have produced such a thing without a computer,” she says. “But it took quite a while typing with two fingers.”

Likewise, her husband John uses the laptop for regular correspondence – including several letters to MPs – as well as Skype network for calls to family, book purchases on Amazon, monitoring ISA offers and keeping in contact with his local doctor. “It means I can order repeat prescriptions without visiting the surgery, and the tablets are delivered to our local pharmacy,” he adds.

Away from the computer, John and Marianne rely on digital terrestrial television for access to rolling news channels and digital radio stations such as BBC7.

While both applaud the speed and breadth of content available through digital technology, they complain it’s not reliable and horribly complicated to move service provider. “Broadband is much more efficient and quicker than the old system,” says John. “But when it breaks down it’s very irritating.”

