Contents

Foreword

Over the past decade, the internet has grown to become a central part of the cultural and economic life of many people around the world. It is a powerful platform for the distribution of services to their intended audiences, spanning the world and connecting a global audience with a globally provided set of content and services, and with one another. The internet's flexibility means it has been an engine for innovation, enabling the development of new businesses and new business models, new content and new communications services; and its openness means it has allowed operators of every scale, from multinationals to individuals, to create and offer content and services as well as benefit from them. Alongside global reach, openness and flexibility, many observers attribute the success and importance of the internet to the limited extent of internet service regulation.

The regulation of internet services is the subject of significant international debate. Consumers expect to be protected from fraud or other forms of harm; and their children protected from inappropriate content. To date, this protection has been provided largely through a framework of domestic and international statutory regulation which has been evolving for decades. However, the global reach and open nature of the internet gives rise to some well-known problems, which cannot be addressed by a translation of existing powers and structures. These problems include the ubiquitous availability of pornography and increased availability of illegal imagery (e.g. violent pornography, child abuse), and easier access to products and services otherwise tightly-controlled like gambling or prescription drugs.

As the UK communications regulator, Ofcom has oversight of the wholesale and retail markets for internet connectivity. We also have a statutory duty to promote media literacy, a role in encouraging audiences to connect to the internet, and in helping them learn how to manage the risks to which they are exposed when online. We therefore have a clear interest in the protection of consumers from harm when they use the internet. Furthermore, the current draft of the EU Audiovisual Media Services Directive proposed an extension of a broadcast-like regulatory framework to audiovisual content delivered in other ways – and might therefore require statutory content regulation to be applied to a broad range of internet services.

This document is a research report intended to inform the debate about the most appropriate ways to address the consumer protection challenges raised by the internet, such as those identified above. It is a broad survey of the key internet consumer protection issues and the national and international approaches taken to tackling those issues across the world. It does not include policy recommendations, though we do comment on the varying success of some of the initiatives adopted.

We can also draw some general lessons from the survey. There is no doubt that consumers will need to bear a greater degree of responsibility when they engage with internet services. Secondly, the broad range of internet services – from e-commerce to VoD to email – will require a broad and flexible set of regulatory solutions. There is no single answer to the issues to which the internet gives rise. However, there are already many factors contributing to consumer protection online, from the application of general law through to initiatives from individual internet players and collective industry bodies like the Internet Watch Foundation. We believe that such self-regulatory initiatives, allied to effective media literacy initiatives and supported by general law, will continue to be the most effective way to deliver consumer protection.

We hope that interested parties across industry, government and consumers will respond to the publication of this report with a continuing and open debate about the challenges to which the internet gives rise. In addressing them, the protection of consumers' security and safety will need to be balanced with the preservation of the internet's potential as a platform for innovation.

David Currie
Chairman

Stephen A. Carter
Chief Executive

Section 1

Executive summary

1.1 As the communications regulator, Ofcom has a number of responsibilities in relation to the internet. We oversee the wholesale and retail markets for internet connectivity. We have a role in encouraging audiences to connect to the internet and in helping them learn how to manage the risks to which they are exposed when online, which arises from our duty to promote media literacy. We therefore have a clear interest in the protection of consumers from harm when they use the internet. Given our responsibility for the UK communications industries, the development of the institutional structures appropriate for the internet will profoundly affect Ofcom.

1.2 Ofcom believes that it would not be appropriate or effective to attempt to translate existing regulatory structures onto the internet. The internet was created as an essentially open access network. The existing lack of regulation has contributed to its very success and the innovation it has engendered. In the future, it will therefore be important to maintain the benefits of this open approach as much as possible in order not to cause undue negative impact on consumers as well as businesses.

1.3 The internet has become an increasingly important part of our daily life. 57% of all UK adults now have access to the internet at home[1]. Electronic communication is an indispensable feature of almost every workplace, and has come to dominate not only our professional interactions but personal ones too. We are increasingly turning to the internet for news and information, as well as for many other services. 82% of online consumers use the internet for sending and receiving email, while as many as 65% now use it to purchase goods and services, and 47% use it for online banking services[2].

1.4 As legitimate use of the internet has grown, so have the scale and impact of its fraudulent and criminal uses. The international nature of the internet has generated new opportunities for consumers but it has also put them within easier reach of those seeking to take advantage of them. The internet has given rise to many new types of crime – for example, identity theft by phishing, malicious virus dissemination via SPAM, and online grooming of children. It has also made it easier for criminals to circumvent judicial systems by taking advantage of the impersonal nature of the internet to misrepresent or disguise their true identity.

1.5 The internet therefore raises important consumer protection issues for governments and policy makers to consider. In order to inform the current debate on how best to tackle them, we believe it would be helpful, for policy makers and the public alike, to present a survey of the key consumer protection issues related to the internet, and the approaches taken to tackling those issues in the UK and internationally.

1.6 In response both to the growing role the internet plays in delivering services to consumers and the risks it exposes them to, there has been an immense amount of activity at national and international levels in developing legislative and regulatory frameworks to deal with internet-specific issues. While some of these efforts have involved attempts to achieve international cooperation and harmonisation of laws,

[1] The Communications Market: Nations and Regions Report, April 2006
[2] Ofcom Residential Tracker, August 2004

many have also been tailored to suit the particular circumstances, and cultural and political norms of local markets.

1.7 From our brief survey of different approaches to regulating some of the key consumer protection issues that the internet raises – such as privacy and security, and protection from illegal or inappropriate content, or from malicious software – we make four observations about the effectiveness of regulation relating to the internet and the services delivered over the internet:

- The attempts at consumer protection on the internet at both national and international level have met with varying degrees of success to date
- Successful consumer protection on the internet has generally involved a much higher degree of co- and self-regulation than has been the case for other media
- Effective consumer protection on the internet requires more significant levels of international cooperation than currently exist
- The internet inevitably places a much greater responsibility on consumers to take action to protect themselves

The attempts at consumer protection on the internet at both national and international level have met with varying degrees of success to date

1.8 The internet is a decentralised "network of networks" containing a number of parallel supply chains involving the physical infrastructure, application and service providers as well as governance structures.

1.9 Regulatory action can be taken at many different levels of the internet value chain. For example, content can be monitored and removed at the level of servers hosting the content; access to certain websites can be prevented at the level of search engines for all users; while controlled access for some users, such as children, can be maintained at the level of internet access at home.

1.10 In cases where effective action can be taken by national ISPs, or consumers have the information as well as relevant skills and tools like software application, actions to increase levels of consumer protection can be quite effective. In other cases, successful action has been more difficult to achieve because it requires cooperation between many different levels of the internet value chain.

1.11 For example, UK consumers now have a generally high level of SPAM awareness and most ISPs offer simple and effective filtering tools which allow users to easily identify and block unsolicited email communications. The problem of SPAM has not disappeared – it is still estimated to account for around 85% of all email traffic and has significant costs for businesses[3] – but there are now more tools available to consumers to reduce the amount of SPAM they receive.

1.12 Despite an increasing number of national and international laws and agreements, internet-related issues remain a serious and growing concern. For example:

[3] Messaging Anti-Abuse Working Group Q4 2005 Report

- The Information Commissioner's Office, the regulator charged with oversight of data protection regulation in the UK, received over 19,000 data protection complaints from the general public in 2004[4]

- Phishing incidents are becoming increasingly common. Globally, the Anti Phishing Working Group reported 16,882 unique attacks in November 2005, up from 8,975 unique attacks launched in November 2004[5]. The UK government's Get Safe Online report estimated the total cost of phishing in the UK reaching £12m[6]

- BT reported in December 2005 that its "cleanfeed" technology blocks an average of 45,000 attempted hits onto illegal child pornography sites each day[7]

- 20% of adverts on a child-orientated games site were promoting gambling services, which would be illegal for their underage viewers to use[8].

Successful consumer protection on the internet has generally involved a much higher degree of co- and self-regulation than has been the case for other media

1.13 The attempts to translate traditional direct regulatory structures onto the internet have for the main part been ineffective at achieving their desired goals. Where action has been effective, both nationally and internationally, it has often involved co- or self-regulatory measures developed with participation from the industry.

1.14 The Internet Watch Foundation (IWF) in the UK is one such example of self-regulation. The IWF operates a hotline for reporting illegal content on the internet. Once content is ascertained by the IWF to be illegal, it issues take-down notices to hosting service providers, when these are based in the UK. Additionally, it supplies ISPs with details of websites containing internationally hosted illegal content, and of online user groups dedicated to disseminating illegal and offensive material. Most UK ISPs have already voluntarily agreed to block those sites and user groups. The IWF has been a successful self-regulatory strategy – in 2005, only 0.4% of potentially illegal child abuse images reported to the IWF were hosted in the UK[9]. However, the international problem remains.

1.15 At international level, industry-led measures have played a significant part in increasing consumer confidence in e-commerce and hence making the internet a more secure place for commercial transactions. For example, data encryption through the https protocol has been widely adopted by online banking and commercial sites, although there remains a need for on-going investments to ensure adequate levels of security. Furthermore, significant efforts have been invested by the industry in marketing its benefits to consumers – today, for example, the padlock symbol is displayed on many browser windows. Though further efforts are needed to ensure that the padlock symbol guarantees adequate levels of consumer protection, its use by e-traders can serve to give consumers the peace of mind necessary to decide to engage in e-commerce.

[4] Information Commissioner's Office
[5] Anti-Phishing Working Group Phishing Activity Trends Report, November 2005
[6] Get Safe Online
[7] BT. See http://www.btplc.com/societyandenvironment/news/showarticle.cfm?articleid=2ab29f02-bd0c-4e0a-952f-60fef2500246
[8] NCH, GamCare, Citizen Card Report 2004
[9] Internet Watch Foundation

1.16 Another example of an international self-regulatory initiative is the Internet Content Rating Association (ICRA). ICRA encourages content providers to self-classify their content using its rating system, which in turn enables end-users to use filtering software to block access to any websites which they deem undesirable based on the rating information. Over 100,000 internet content providers have already self-labelled using ICRA's rating system, including Microsoft, AOL, T-Online and Hustler. However, the vast majority of internet content is still not labelled.

Effective consumer protection on the internet requires more significant levels of international cooperation than currently exist

1.17 The internet has fostered unprecedented levels of exchange of information, services and trade across countries. This has been made possible by the international nature of the internet both in terms of its infrastructure, and in terms of content and reach. However, the internet's international nature also means that regulatory action at certain levels of the value chain can only be taken at international level. While measures taken at the content access level, for example software applications, are most effectively achieved via ISPs, and therefore at national level, any action at the level of say hosting, would require international cooperation.

1.18 Additionally, lack of international cooperation on laws and measures to tackle criminal activity on the internet can render national laws ineffective, however stringent, because criminals can simply move their operation to countries where minimal protections exist.

1.19 International cooperation on internet-related issues has been growing. For example, the 2001 Council of Europe Convention on Cybercrime was the first international treaty to address cybercrime specifically. Signatories to the Convention are required to enact national laws criminalising four categories of computer related crime: fraud and forgery, child pornography, copyright infringements, and security breaches such as hacking, illegal data interception, and system interferences that compromise network integrity and availability.

1.20 To date, however, much international cooperation has lacked the enforcement means to make it effective. Most efforts involve greater knowledge sharing and information on best practice but there have been very few instances of any action taken against perpetrators.

1.21 Part of the reason for the lack of success in acting against perpetrators is the difficulty in achieving agreement on the appropriate action to be taken. Variations between cultural and political norms, as well as different stages of market development and levels of resources available to enforcement agencies, have often meant that international agreement is only possible at the level of the lowest common factor.

The internet inevitably places a much greater responsibility on consumers to take action to protect themselves

1.22 The international nature of the internet means that there are inherent limits on the regulatory action taken at a national level. In contrast to the closed access platforms, the open access nature of the internet means that internet service providers act primarily as conduits for information and do not exercise editorial control over the content that flows over their networks. As a result, consumers will inevitably have to take a much greater responsibility to take action to protect themselves both from unwanted content and services, and from the various types of cybercrime.

1.23 Several information and media literacy initiatives have been developed to date to educate consumers about the dangers of the internet and help them understand the consumer protection tools that are available to them. In the UK, websites such as Get Safe Online, a public-private partnership initiative – see www.getsafeonline.org – and www.consumerdirect.gov.uk (run by the OFT) provide information and advice on internet safety and consumer rights.

1.24 Additionally the development of quality seals aims to help consumers recognise which vendors have committed to following a code of conduct in relation to commercial transactions on the internet. For example, quality seal systems are in place in the UK (TrustUK), France (L@belsite), Germany (Trustedshops) and Japan (Japan DMA), while the Global Trustmark Alliance promotes the use of quality seals at an international level.

1.25 In the future, we believe that consumers will have to assume greater responsibility for protecting themselves online if they are continue to enjoy the benefits of plurality and diversity of content and services the internet brings. To be able to do that, the consumers will need to have access to trustworthy information and advice, and affordable, easy-to-use technological tools. Therefore, it will be crucial to foster the further development of end-user education and empowerment while addressing the needs of vulnerable groups.

Next steps

1.26 Ofcom intends this report to become the first in a series of regular surveys of international approaches to regulation and the internet, which will allow it to track the emergence of new regulatory tools and frameworks, and the development of new institutional structures dealing with the internet as a communications platform.

1.27 Parallel to this survey, Ofcom is undertaking a number of projects assessing the impact of increased convergence in communications markets, and identifying any changes in the regulatory approach that may be required as a result of convergence. They include:

- Convergent media: looking at the structure of content regulation as similar content is increasingly delivered over multiple platforms
- Approaches to regulation: looking at the major regulatory and institutional questions arising in other countries, and how those are being addressed
- Media literacy and digital consumer: research projects to understand the way in which different types of consumer understand and interact with digital media.

1.28 Finally, while we do not draw specific policy recommendations from this survey, we hope it will open a debate with and amongst interested parties on the appropriate response to the consumer protection challenges posed by the internet.

Section 2

Introduction

Evolution of the internet

2.1 In a very short time, the internet has evolved from being an innovative technological tool used initially by the military but then mainly by academia, to being a part of our everyday life. 57% of all UK adults now have access to the internet at home, compared to 65% with digital TV services and 80% with mobile phone services[10]. Broadband penetration currently stands at 68% of those with internet access at home and 39% of all UK homes[11].

2.2 The internet is not only a source of an immense amount of information. Rapid development of new web technologies that are simple and cheap to implement has greatly enriched users' experience of the internet:

- Increasing download/upload speeds have enabled greater user interaction and improved users' online experience by allowing fast multimedia services
- New technologies such as XML and Ajax have enabled easier and faster service composition and innovation
- Large communities of developers have formed that produce innovative open source software and often create niche markets or disrupt major players
- Many users have become more experienced and now understand better how to utilise the internet thus driving demand for services that better suit their needs.

2.3 The evolution of the internet as a computing and service platform rather than simply a distribution medium has opened up many new opportunities for users. It has given them greater control over the content and services they receive by enabling them to customise their online experience to suit their tastes and interests. It has enabled them to form online communities and share content, and given them an ability to participate in the development of new services.

2.4 The internet is also used increasingly as a distribution platform for services that were traditionally delivered on other communications networks. While 82% of online consumers use the internet for sending and receiving email, 65% now report using it to purchase goods and services, and 47% report using online banking services[12].

2.5 Additionally, a growing number of media companies as well as internet service providers are offering more choice to consumers through audio-visual content delivered over the internet, while Voice over Internet Protocol (VoIP) services have delivered consumer benefits through lower prices and increased competition in voice markets.

2.6 The impact of the internet on offline markets is significant. Increasingly, free community-based amateur online projects are competing directly with professional

[10] The Communications Market: Nations and Regions Report, April 2006
[11] Ofcom Communications Tracking Survey, Q4 2005
[12] Ofcom Residential Tracker, August 2004

commercial services. Web logs, with their online editing functionality and minimum technological requirements, have resulted in a tremendous increase in user-generated content and have contributed to media fragmentation.

2.7 Internet technologies have also opened up new opportunities for marketers. As a reflection of the potential advertising power of the internet, the UK internet advertising spend for 2005 is estimated at £1.13bn, representing a 73% year-on-year increase compared to the total UK advertising spend increase of 2%[13].

Consumer protection challenge

2.8 The rise of the internet has undoubtedly brought about many consumer benefits and the internet continues to offer enormous potential for education, entertainment and business. However, the increasing convergence of communications markets has also introduced new challenges for policy makers and regulators, especially in the area of consumer protection.

2.9 For example, the international nature of the internet, and the opportunity it gives users to remain anonymous, have made it easier for users to disseminate criminal and/or inappropriate content, such as for example child pornography or advice on how to engage in harmful activities. It has also given rise to new types of crime, for example, phishing and the online grooming of children. These types of crime are of a substantial scale and many are growing fast:

- According to all estimates, SPAM still accounts for c.85% of all email traffic[14]
- In the UK, banks' losses from internet banking fraud more than trebled last year to £14.5m for the six months to June 2005[15]
- According to the report published by the Anti-Phishing Working Group (APWG), an industry consortium that provides information on phishing trends, the number of unique email-based fraud attacks detected in November 2005 was 16,882 - almost double the 8,975 attacks launched in November 2004[16].

2.10 Ofcom believes that it would not be appropriate or effective to attempt to translate existing regulatory structures onto the internet. The internet was created as an essentially open access network and its architecture is often not suited to the methods employed traditionally to regulate communications markets.

2.11 Part of the reason why the use of the internet has grown so rapidly is because it has operated in an environment effectively devoid of regulation which has stimulated innovation in products and services. Going forward, it will therefore be important to maintain the benefits of this open approach as much as possible in order not to exercise undue negative impact on consumers as well as businesses.

2.12 Additionally, the global nature of the internet often makes it very difficult to implement direct regulation. Most regulatory frameworks are developed and applied within national boundaries and can therefore easily be avoided by those who operate across national borders. Any measures that fail to take into account the global

[13] World Advertising Research Centre
[14] Messaging Anti-Abuse Working Group Q4 2005 Report
[15] Association for Payment Clearing Services (APACS)
[16] Anti-Phishing Working Group Phishing Activity Trends Report, November 2005

aspects of the provision and consumption of internet content and services are bound to be ineffective.

2.13 Notwithstanding the above, the internet raises important consumer protection and competition issues for the governments and regulators to consider. There are likely to be areas where some form of constraints on the internet may well be appropriate as well as effective. However, any regulatory intervention on the internet would require a different conceptual and institutional approach to that applied today. Rather than extending direct statutory regulation to the internet, this new approach would require a greater use of co- and self-regulation, as well as much greater international cooperation.

2.14 For the purposes of this report, we define direct co- and self-regulation as follows:

- **Direct regulation**: Where a statutory body is empowered by law to develop its own regulations which it maintains, monitors and enforces
- **Co-regulation**: Where a body with statutory regulatory authority delegates to the relevant industry responsibility for maintaining and applying a code of practice that the statutory regulator has approved. The statutory regulator is responsible for overseeing the effectiveness of co-regulation, and retain powers to intervene where necessary
- **Self-regulation**: Where a group of firms or individuals exert control over their own membership and their behaviour. Membership is voluntary and participants draw up their own rules using tools such as codes of conduct to define good or bad practice as well as technological solutions and standards. Members take full responsibility for monitoring and compliance without reference to a statutory regulatory authority.

Ofcom's statutory duties

2.15 The Communications Act 2003 gives Ofcom specific responsibilities across UK communications industries including television, radio, telecommunications and wireless communications services.

2.16 Under Section 3(1) of the Communications Act 2003, Ofcom's principal duties, in carrying out its functions, are to:

- Further the interests of citizens in relation to communications matters, and
- Further the interests of consumers in relevant markets, where appropriate by promoting competition.

2.17 Additionally, under Section 11 of the Communications Act 2003, Ofcom is required to bring about, or to encourage others to bring about, a better public understanding of:

- The nature and characteristics of the material published by means of the electronic media
- The processes and systems by which access to such material is or can be regulated, and
- The systems which allow users to control what material they receive.

2.18 Ofcom is also required under Section 11 to encourage the development and use of technologies and systems for regulating access to such material, and for facilitating control over what material is received.

2.19 Ofcom is responsible for the economic regulation of the markets for internet connectivity, and regulates communication services close substitutes of which are increasingly delivered over the internet. Given Ofcom's responsibilities for the UK communications industries, the development of the institutional structures that are appropriate for the internet will profoundly affect Ofcom, even if Ofcom continues to have a limited formal role in this area.

The objectives of the report

2.20 Ofcom's recent Media Literacy report suggests that levels of concern about the internet are relatively high in comparison to other platforms. 70% of users reported concerns about what is on the internet, with 55% concerned about offensive content and 28% concerned about risks to personal privacy. This compares to 46% who reported concerns about what is on TV and 9% who reported concerns about what is on the radio[17].

2.21 Furthermore, there is evidence that internet literacy is still relatively limited. While 86% of users reported confidence in ability to use email and 81% reported confidence in using the internet to find the latest news, the reported confidence in blocking email SPAM and computer viruses was only 58% and 57% respectively. And while 54% of users were happy to enter personal email address on the internet, only 28% of users said they were likely to disclose credit card information on the internet[18].

2.22 Given the high level of public concern over the dangers that the internet has given rise to, and Ofcom's clear interest in the protection of consumers from harm when they use the internet, we believe it would be helpful, for the policy makers and the public alike, to present a survey of the key consumer protection issues related to the internet and the approaches taken to tackling those issues in the UK and internationally.

2.23 This report does not cover every consumer protection issue raised by the internet. For example, we have not commented on debates about redress and access to dispute resolution systems, or about universal service obligations which is an issue that Ofcom has worked on extensively. In this report, we focus on many of the issues that have generated the most debate.

2.24 In particular, we thought it is important to outline the measures that have already been taken, both nationally and internationally, in addressing these issues and the bodies responsible for them, and to draw lessons, where appropriate, from approaches taken by other countries.

2.25 The key issues we focus on in this report are:

- Protection of personal data
- E-commerce

[17] Ofcom Media Literacy Audit 2006
[18] Ofcom Media Literacy Audit 2006

- Content and contact
- Malicious computer activity

2.26 The rest of this document is structured as follows:

- Section 3 describes the structure of the internet, the players in the value chain and the potential roles they are able to play in internet regulation
- Section 4-7 discusses consumer protection issues detailed above

Next steps

2.27 Ofcom intends that this report will become the first in a series of regular surveys of international approaches to regulation and the internet, which will allow it to track the emergence of new regulatory tools and frameworks, and the development of new institutional structures dealing with the internet as a communications platform.

2.28 Parallel to this survey, Ofcom is undertaking a number of projects assessing the impact of increased convergence in communications markets, and identifying any changes in the regulatory approach that may be required as a result of convergence. They include:

- Convergent media: looking at the structure of content regulation as similar content is increasingly delivered over multiple platforms
- Approaches to regulation: looking at the major regulatory and institutional questions arising in other countries, and how those are being addressed
- Media literacy and digital consumer: research projects to understand the way in which different types of consumer understand and interact with digital media.

2.29 Finally, while we do not draw specific policy recommendations from this survey, we hope it will open a debate with and amongst interested parties on the appropriate response to the challenges posed by the internet.

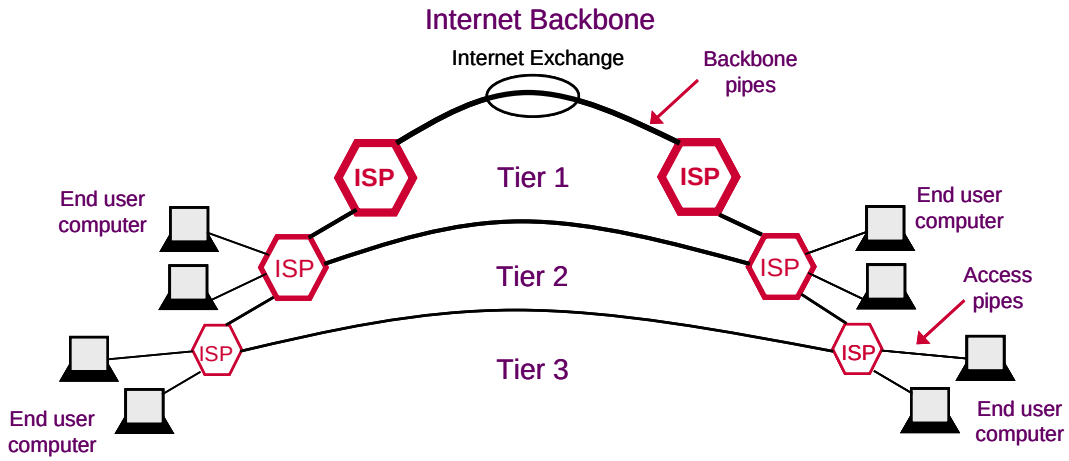
Section 3

The structure of the internet

3.1 The internet is a global 'network of networks'. Individual computer networks, each potentially containing thousands of different computers, are interconnected, allowing each computer to communicate with all the others. To enable each computer to communicate with all the others ones, network operators have adopted a universal addressing system and a set of standardised communications protocols. The addressing system uses Internet Protocol (IP) addresses and domain names (explained in more detail below). The communication protocols, or rule sets, make the different networks interoperable, ensuring they can communicate with one another. With unique addresses and shared protocols, any Computer *A* on Network X is able to transmit data to any Computer *B* on Network Y.

3.2 Internet Service Providers (ISPs) – the network operators – largely work in a hierarchical architecture, illustrated in Figure 3.1. There are three tiers of ISP, each of which will typically have peering and paid-for links with other ISPs. ISPs in the same tier peer with one another - exchanging data between each other's customers freely and for mutual benefit. ISPs in the higher tiers sell internet connectivity to those in the tier below.

Figure 3.1 Schematic overview of the internet



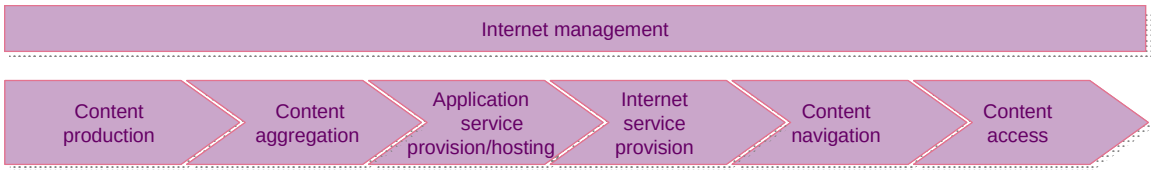
3.3 Tier 1 ISPs, the largest, form the backbone of the internet and sell internet backbone connectivity to tier 2 ISPs. Tier 2 ISPs may peer, and sell internet connectivity to Tier 3 ISPs as well as to end users. End users usually connect to the internet through Tier 2 and Tier 3 ISPs.

3.4 However, this hierarchical model is gradually being replaced with a more decentralised one, as result of new application demands and the emergence of new models for interconnection. In the more decentralised structure, there is more peering between ISP's of the same scale and between those of different scale – across the historic tiers. This means that the relative importance of the Tier 1 providers is falling – and opportunities to control the internet by focusing on Tier 1 providers are similarly being reduced.

3.5 The structure of the internet for service delivery can be represented as a two-layer value chain, comprising seven core elements (Fig. 3.2). There is a single management layer, made up of the players who provide governance, oversee

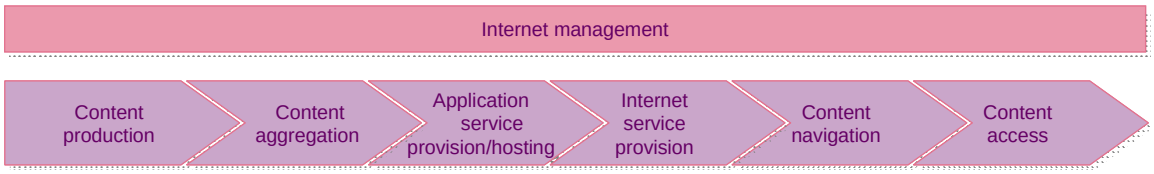
standards development and addressing, and support the other six activities across the value chain. There are six distinct activities supported by the management layer, which collectively enable the direct delivery of internet services.

Figure 3.2 The seven core elements in the two layers of the internet value chain



3.6 This chapter examines each of these value chain activities, giving: (i) a description of the activity's role in creating the internet and (ii) an overview of the ways in which the players in each stage of the value chain can potentially contribute to consumer protection on the internet. In reality, commercial operators often span more than one activity in the value chain. Examples of players involved in the internet value chain are provided in the summary table at the end of this section.

Internet management layer



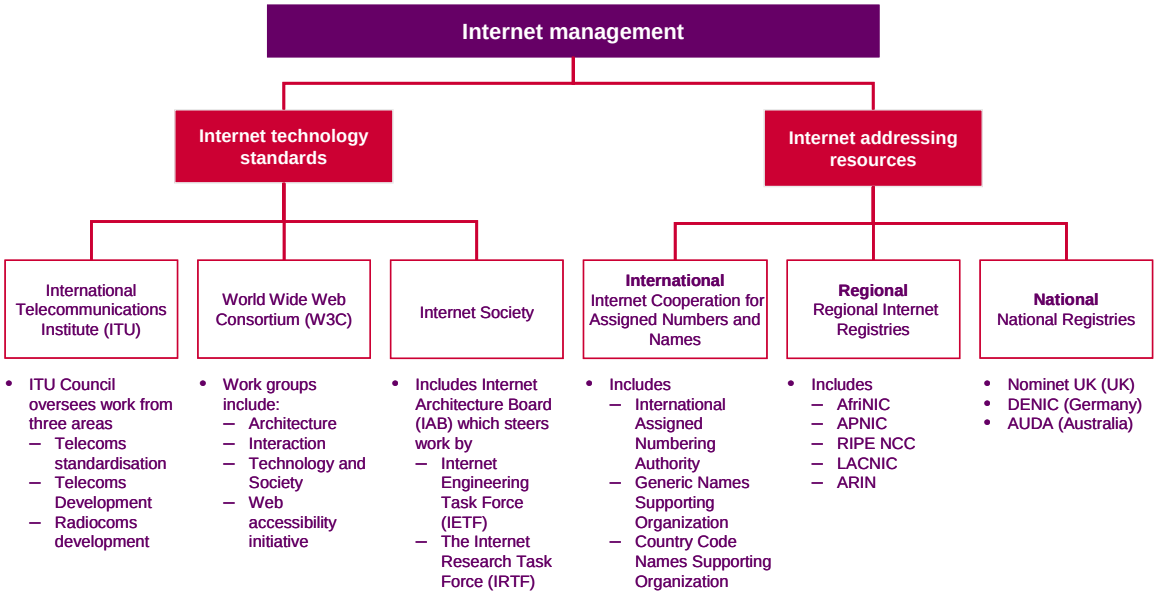
The role in creating the internet

3.7 The internet management layer refers to the international, regional and national bodies which manage the technology and addressing system which supports the internet.

3.8 In terms of technology, these bodies play a role in ensuring that the standards that support the internet (e.g. transport protocols such as TCP and internet languages such as HTML) are interoperable and work together. Examples of such bodies include the International Telecommunications Union (ITU), the World Wide Web Consortium (W3C) and the Internet Society.

3.9 Organisations involved in internet addressing play a role in managing the global addressing system which enables users to locate sites with specific content and services and locate individual computers on any given network. Examples of such bodies include the Internet Corporation for Assigned Names and Numbers (ICANN), Regional Internet Registries (RIRs) and Nominet.

Figure 3.3 Illustrative structure of the internet management layer – key bodies



3.10 Briefly, the internet addressing system has two parallel schemes

- IP addresses
- Domain names

IP addresses

3.11 The IP addressing system is based on either a 32-bit or 128-bit number (referred to respectively as IPv4 and IPv6 addresses). The first part of the number identifies a specific network on the internet (e.g. BT) and the second part identifies a specific node or terminal on that network (e.g. a computer in a BT subscriber's home). In this way, every computer connected to the internet could have its own unique IP address.

3.12 In practice not every computer with an internet connection has a unique IP address. Many ISPs do not use static IP addressing, under which a permanent IP address is assigned to every computer on the network. Instead, they use 'dynamic addressing', which allows the provider to assign a computer an IP address each time it is connected to the internet. This allows the ISP to use fewer IP addresses for a given group of computers.

3.13 Currently, Regional Internet Registries (RIRs) are responsible for allocating IP addresses to network operators. In Europe, this is done through Local Internet Registries (LIRs), all of whom are members of the Réseaux IP Européens Network Coordination Centre (RIPE NCC), an independent organisation funded by membership fees. The allocation of IP addresses is free, but requires an organisation to be a member.

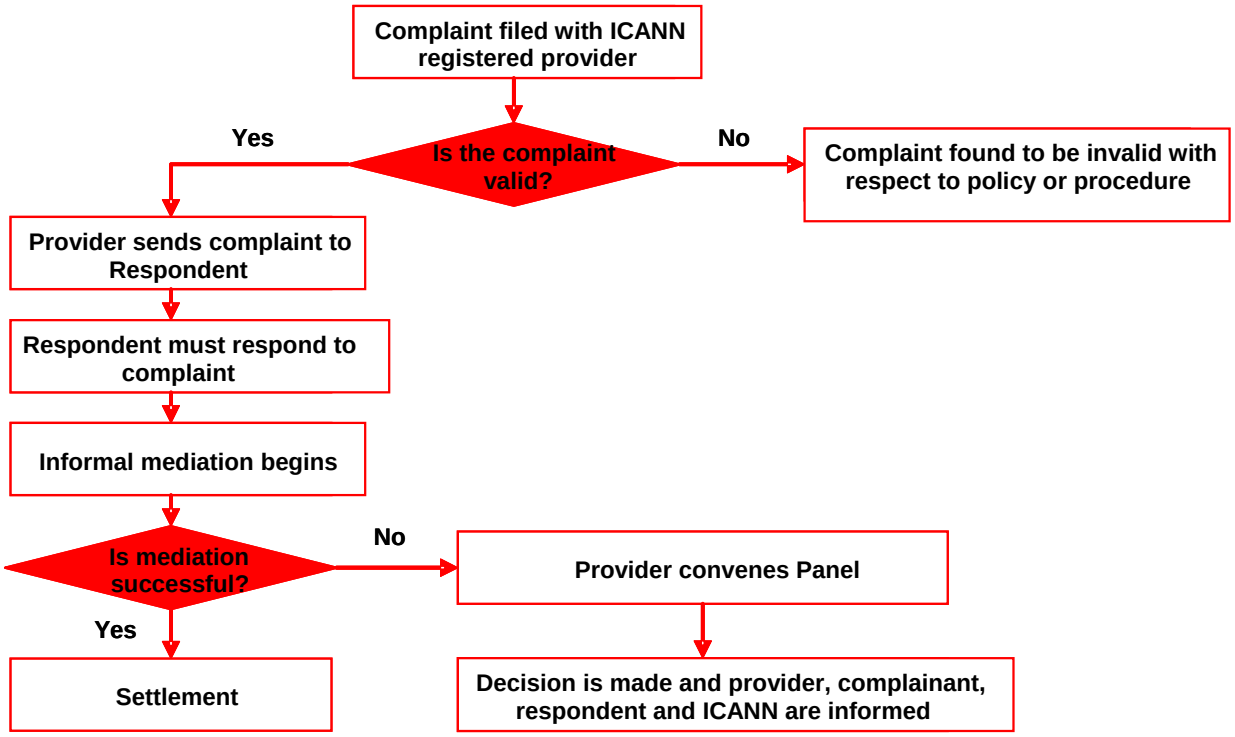
3.14 The current IP address space (over 4 billion addresses) is divided and allocated to operators in blocks, with the size of the block depending on the size of the ISP's – that is, on the number of end user computers attached to the operator's network. Once allocated a block of IP addresses, ISPs can either statically re-allocate the addresses to label individual end user computers, or dynamically allocate the addresses to individual user internet sessions on their network.

Domain names

3.15 The second element of the addressing system, the domain name system, uses strings of memorable letters as an address for a specific website (e.g. www.ofcom.org.uk). Domain names are associated with a particular IP address, and it is possible to have multiple domain names associated with the same IP address. The association of domain name and IP address links a website to its physical location on a computer, on a network.

3.16 The domain name system (DNS) is managed, at a high level, by the Internet Corporation for Assigned Names and Numbers (ICANN). ICANN maintains the allowed list of 'generic top level domain' names, of which there are currently ten: .com, .biz, .pro, .aero, .org, .museum, .net, .info, .name and .coop. To purchase a domain name, a user must go through a Registrar, who sells available names on a competitive basis. ICANN maintains a list of accredited Registrars and approved administrative dispute resolution service providers; these latter groups provide mediation services in cases of domain name disputes. ICANN has also established a strict dispute resolution procedure which is outlined below.

Figure 3.4 Overview of dispute resolution process as established by ICANN



3.17 There are also country level top level domain names, such as .uk, .fr and .de and these are usually managed by an independent, non-profit organisation based in the relevant country. In the UK, the .uk domain name is managed by Nominet UK. The function of these organisations mirrors that of ICANN, but they operate at a national level rather than an international one.

Roles played in supporting consumer protection

3.18 The first element of the internet management layer, comprising the bodies which manage the technology standards which supports the internet, has a relatively limited

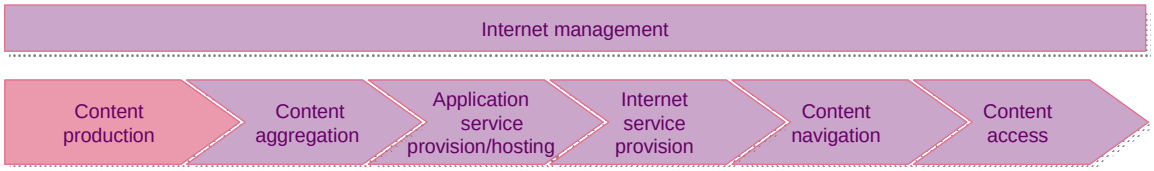
direct role to play in supporting consumer protection. In the majority of cases, such bodies are "service neutral" in the way they carry out their functions: their primary role is to ensure that the internet works physically and technologically, without regard to the qualitative nature of content or service. However, these bodies could have a role to play in supporting the development of technologies that deliver consumer protection on the internet, for example, SPAM filters or encryption protocols for secure data transfer. Their involvement could range from sharing best practice, conducting research, and producing publications to bringing together groups of experts to solve a specific issue.

3.19 The second element of the management layer concerns the addressing system for the internet. Again, IP address management has a limited role to play in consumer protection as its main focus is on ensuring the integrity of IP addresses and the databases that store them. However, the domain name system could play a substantial role in helping manage consumers access to content, for example by creating top level domain names associated with certain types of content and applications. There are two recent examples of proposals to do so:

- xxx: A proposal to group together pornography sites under one top level domain, which would make it easier for users and filtering technologies to identify and/or block sexually explicit content. ICANN gave this proposal a preliminary approval in June 2005 but then reversed its decision under strong pressure from a number of governments. Following a period of heated debate ICANN finally rejected the proposal in May 2006.

- Kids: A proposal to create a safe internet space for children under a .kids domain name, which would only contain content and applications suitable for children. This proposal has stalled due to fears that it would not be possible to ensure that no inappropriate content was posted under the domain, and concerns about the level of monitoring that would be required to ensure suitability of content for children.

Content production



The role in creating the internet

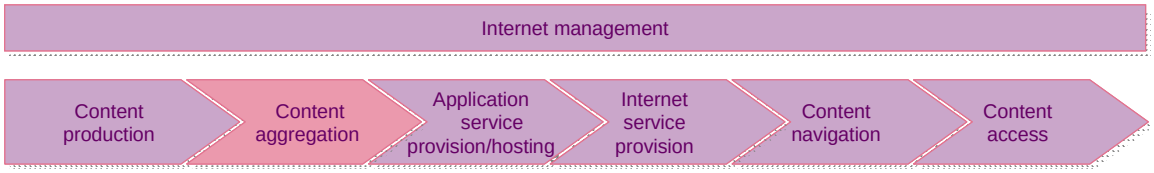
3.20 Content producers commission, produce and own the original copyrights to the content available on the internet. Content producers on the internet not only include the traditional content producers like Universal Studios, Disney and BBC but also a whole range of new players including individual artists and internet users.

Roles played in supporting consumer protection

3.21 Content producers can play a significant role in delivering consumer protection on the internet. Most importantly, they can label their content and insert tags (metadata) that can be used to filter the content. Labelling entails packaging content with information about the characteristics of the product or service. Examples include easily understood graphics, plain English descriptions or the classification and rating systems used in cinemas. Metadata tags provide content information which is not

presented to the user but which can be used to filter out unwanted or inappropriate material.

Content aggregation



The role in creating the internet

3.22 Content aggregators purchase content and negotiate rights deals from multiple content producers. They also encode, manage and package the content for distribution downstream. Examples of content aggregators on the internet include internet brands such as iTunes, Yahoo! and AOL; and traditional aggregators such as Sky or the BBC. Content aggregators may differentiate themselves by focusing on particular content, as iTunes initially did with music, or may aggregate a wide range of content as AOL does.

Roles played in supporting consumer protection

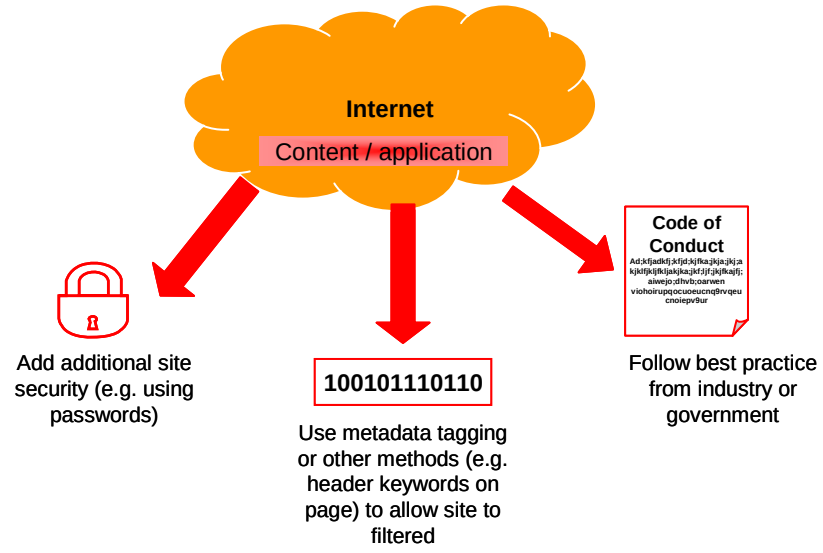
3.23 Content aggregators can play a significant role in supporting consumer protection, as they are responsible for the material they offer and also play a role in drawing together large numbers of users into a single content environment.

3.24 Firstly, content aggregators are able to manage their users' access to the content they offer. This can be achieved a through the use of website security tools (e.g. passwords, subscription, age verification mechanisms such as credit cards checks etc.) or on a geographic level, using a procedure called IP-blocking. With IP blocking, the website will restrict access to users with a particular range of IP addresses associated with a particular territory (e.g. all UK IP addresses are blocked).

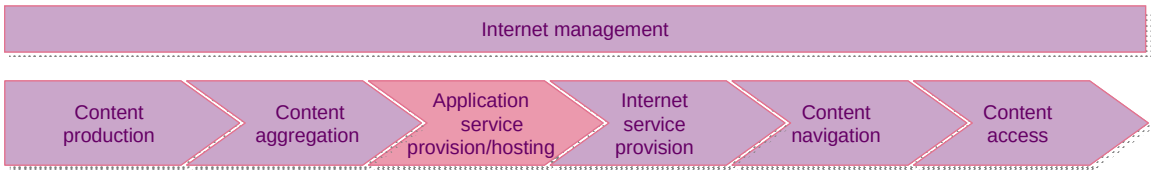
3.25 Secondly, content aggregators can classify their content or make it easily filterable or searchable by software – making it easier for users to locate what they want and avoid what they do not want.

3.26 Finally, as central points for audiences, content aggregators can contribute to consumer protection by employing the relevant industry best practices – for example using secure payment methods for commercial sites, publishing and adhering to privacy policies, or providing opt-out mechanisms for software downloads, advertisement or SPAM to users.

Figure 3.5 The main regulatory roles that can be played by the content aggregator



Application service provision/ hosting



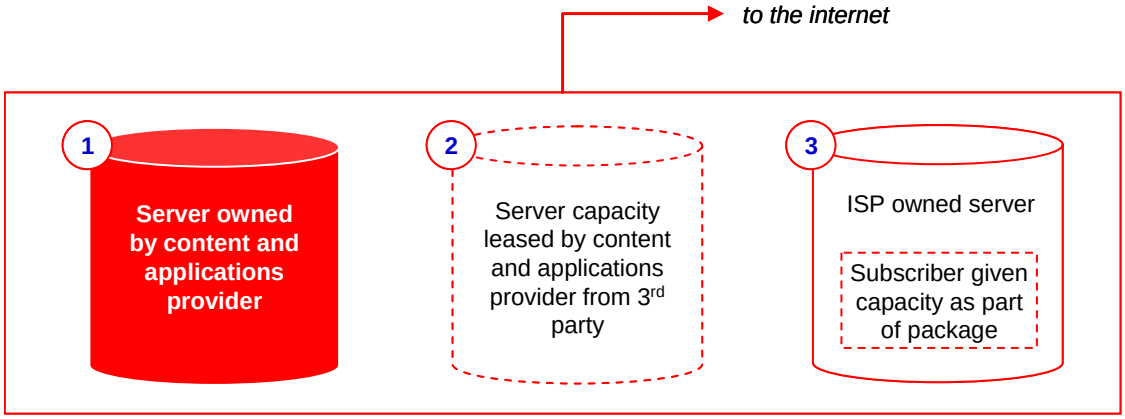
The role in creating the internet

3.27 All content and applications that can be found on the internet must be hosted on an internet-connected server. This can be done in three different ways:

- The internet content producers or aggregators own their own servers and either maintain their own high-bandwidth connection to the internet (e.g. Google owns its own server farms which support its search engine) or co-locate their server at an exchange point
- The internet content aggregator or producer leases a server from a specialist provider, who will also provide a connection to the internet (e.g. BBC Online outsources the provision and maintenance of the servers hosting its websites to Siemens Business Services)
- The internet content aggregator or producer shares servers provided by a third party. This would be the case for most small and medium aggregators or individual producers. The majority of personal websites are hosted by ISPs, with server capacity being provided as a value-added service bundled into a monthly internet package.

3.28 These methods are shown in the diagram below.

Figure 3.6 Schematic diagram showing three different hosting situations



Roles played in supporting consumer protection

3.29 The role that can be played by content and application hosts in supporting consumer protection varies between the three different hosting models described above. In the first case, where the content aggregator or producer provides their own hosting, there is no specific role - beyond those of the content producer and content aggregator, described above. However, this is not the case for the other hosting models.

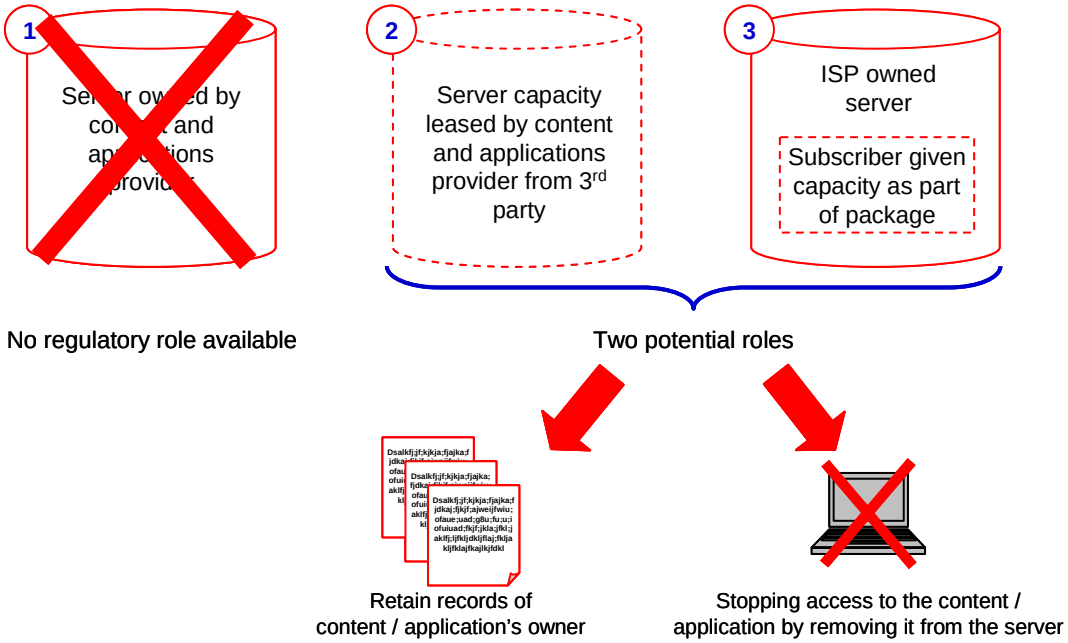
3.30 In the case of the second and third hosting model, the host acts as an intermediary between the content aggregator or producer and the user. In this way the host has control over content and applications on its servers, and can remove them where these are illegal or do not comply with the hosting providers' policies (e.g. some providers do not wish to host legal pornographic content).

3.31 However, hosts are not responsible for monitoring the material they host and cannot determine in advance whether the material they are hosting should be offered on the internet. This means that they will remove content when only they are alerted to the fact that it is illegal or otherwise in breach of their policies.

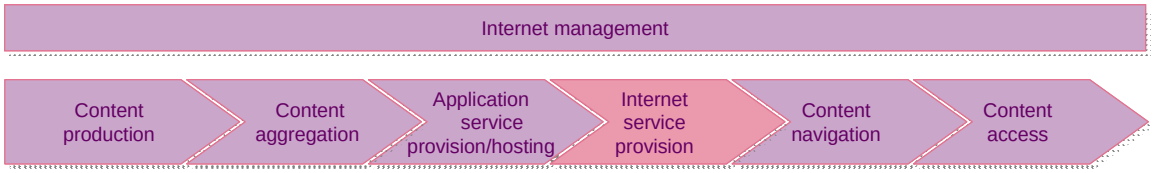
3.32 The other area in which hosts can help to secure consumer protection is through their data records. Content producers and aggregators have a billing relationship with the hosting providers from which they lease capacity. The hosting provider will therefore have some relevant records – for example names, addresses or other details - for the content and applications sets which they host. These records can potentially be used to track down content and applications producers and aggregators involved in illegal activities by law enforcement agencies.

3.33 These two regulatory methods are drawn schematically in the diagram below:

Figure 3.7 Schematic diagram of the two regulatory roles played by the hosting layer



Internet service provision



The role in creating the internet

3.34 The Internet Service Provider (ISP) provides internet access that enables individuals, businesses and institutions to connect to the internet. The ISP may either own or procure the physical access facilities from an access provider. In order to connect to the internet, an ISP may interconnect and exchange traffic with other ISPs in the same tier or may purchase internet connectivity from a bigger ISP i.e. from a higher tier level. The biggest ISPs interconnect at exchange points and form the internet backbone. The internet backbone infrastructure is owned by internet backbone providers. It is spread across the globe and, as such, is not provided by any one player or nation.

3.35 The ISP owns the relationship with the customer under a commercial agreement that defines among other things how the customer may use the connection (e.g. X data downloads a month at Y speed etc.).

Roles played in supporting consumer protection

3.36 ISPs can play a key role in supporting consumer protection. They ultimately control all content entering a user's computer or leaving it to reach the internet. In practical terms, this enables them to restrict access to specific sites or services, as long as the ISP is able to identify the material to be controlled. This is of significant value in some instances: for example, the Internet Watch Foundation provides a global database of IP addresses where illegal content is hosted. UK ISP's use this database to block their subscribers' access to the illegal content.

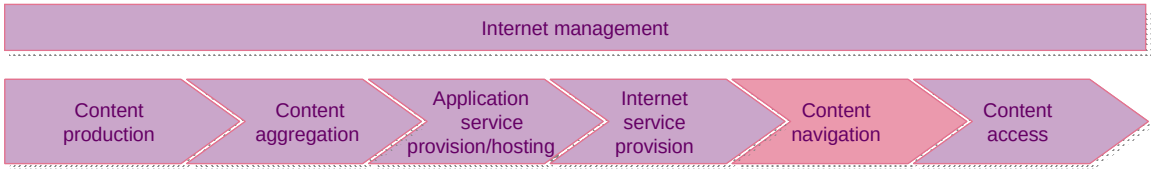
3.37 However, this cannot easily be translated into complete control of the products and services individuals are accessing: doing so would entail being able to classify all of the products and services offered on the internet. Although there is a broad range of filtering tools available, none can guarantee either that all undesired content will be captured ("underblocking"), nor that some appropriate content will not be incorrectly stopped ("overblocking"). Furthermore, there is considerable sensitivity over the extent to which ISP's should themselves seek to monitor and restrict access to the whole internet.

3.38 ISPs also have a direct relationship with subscribers, placing them in a strong position to educate their customers, and to offer them access to appropriate filtering technologies. These tools should help users manage their access to the internet - and that of others in their homes.

3.39 Backbone ISPs can play a role though their control of the main interconnects or the exchange points. At these points, a large ISP has control of all the internet traffic which enters and leaves their network and can restrict the flow of data as they see fit. China's 'Golden Shield' incorporates this approach, placing site/content blocking tools at the backbone layer, potentially preventing all internet users in China from accessing certain sites. A major network operator can block the access of large chunks of the audience to certain sites - as well as preventing traffic sent from their users from leaving their network.

3.40 As for smaller ISP networks, backbone layer filtering cannot deliver complete control of the content because of the continued proliferation of new services and service providers, and the challenge of classifying all content correctly.

Content navigation



The role in creating the internet

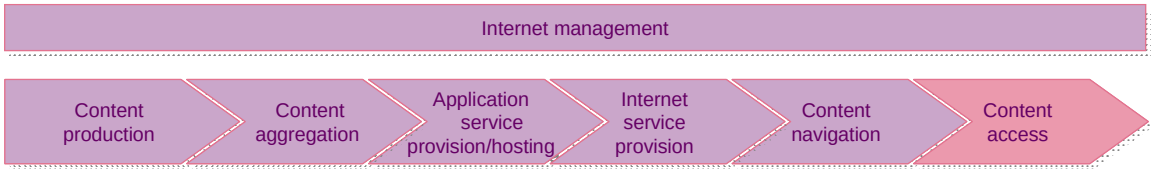
3.41 Content navigation, which includes the use of search engines, directories, online communities and peer recommendation tools, plays a vital role in facilitating users' access to relevant and interesting content and applications. Search engines allow users to search the internet using keywords - words that users anticipate best describe the content and match the tags used by authors to help classify their particular content. Directories classify, group and cross reference the vast amount of internet content so as to enable users to find the content they want or need. Some online communities locate and share links to content which reflects their collective interest.

Roles played in supporting consumer protection

3.42 Content navigation elements are able to play several different roles in supporting consumer protection. For example, using directory navigation enables users to focus their exploration of the internet on defined categories, potentially reducing the risk of exposure to undesired or inappropriate content.

3.43 Similarly, search providers can offer filtered propositions to their users: Google enables its audiences to use a SafeSearch tool. This feature aims to control the search results being returned to the user, according to two sets of SafeSearch criteria. At one level of safety Safesearch aims only to control access to "explicit images" when searching for images (though "explicit" is not further defined); a more restrictive setting aims to block sites with explicit images from appearing in response to image and to ordinary web searches.

Content access



The role in creating the internet

3.44 Content access refers to the software and the underlying hardware that provides an interface for users to access content and applications hosted on the internet. The software and underlying hardware will repackage, interpret and compose the content and applications elements that arrive at the connected end user terminal ready for use or consumption by the end user. For example, internet browsers such as Internet Explorer or Mozilla Firefox enable users to browse and view different websites; email applications such as Outlook or Lotus Notes allow users to write, send and receive emails; while hardware graphics cards enable the composition of multimedia and high quality graphical content.

Roles played in supporting consumer protection

3.45 The main potential role for consumer protection at the content access level is through the use of filtering tools. Specialised software can be installed on a user's computer which can filter and block content according to a range of criteria, and restrict the ability of viruses and spyware to be installed on the terminal. The installation and use of such tools represents an important element of the internet regulatory landscape, although, as noted above, there are persistent concerns over the risks of over- and underblocking.

3.46 Much of the emphasis of recent regulatory efforts has concentrated on end users, either as persons liable for the content and applications they provide, or as the target of media literacy initiatives (many of which are discussed in the main body of this report). The ability of internet users to exercise control over the content they access depends on their having sufficient understanding and knowledge of the tools that are available to them for this purpose. For that reason, media literacy schemes are an essential part of any efforts to ensure that consumers are protected on the internet. Ensuring that consumers are informed about the risks they face and the ways in which they can mitigate these risks is a particularly powerful means of securing consumer protection.

Summary

3.47 The exhibit below summarises the different roles within each stage of the internet value chain, and outlines their potential role in regulating the internet. It also includes examples of players for each part of the value chain.

Table 3.1: The structure of the internet – summary

Value chain element	Core activities	Potential consumer protection roles	Example players
Internet management	• Allocation of IP addresses and overall management of domain name system (DNS) • Selling of domain names to internet content and applications providers • Development and establishment of standardised protocols	• Creation of top level domain names restricted to specific types of content and applications • Formation of technical working groups and forums dedicated to sharing best practice and developing technical solutions	• ICANN • Registrars (e.g. Verisign) • International Telecommunications Union (ITU)
Content producers	• Content producers commission, produce and own the original copyrights to the content available on the internet.	• Labelling and tagging	• Studios e.g. Universal Studios, Disney • Traditional content producers: BBC • Individual artists
Content aggregators	• Content, applications and services	• Establishing additional security measures on sites (e.g. subscription/passwords) • Maintaining lawfulness on sites and adhering to 'best practice' as proscribed by a specific industry	• Commercial services: iTunes, Yahoo!, Google • New players: BBC online • Traditional Content Aggregators: Sky
Application service provision/ hosting	• Hosting of web content, services and applications on networked servers. Can be: • Co-located: on own server • Dedicated: hosted on a leased server • Shared: hosted on a shared server	• Maintaining accurate records of their hosting clients • Removing content and applications from their servers when necessary	• Co-located: Google, Amazon • Dedicated: BBC (on Siemens-owned and maintained servers) • Shared: Individual consumers share space on AOL server as value-added-service
Internet service provision	• Physical and commercial access to the internet, via an access provider or private line, from an individual home	• Blocking user access to specific sites • Maintaining accurate records of user personal details • Monitoring and recording user traffic details • Providing information about 'safe surfing' and filtering technologies • Blocking access to certain websites to all users on their networks	• Physical access provider: BT • Commercial ISPs: BT, Wanadoo, AOL, Tiscali
Internet backbone ISPs	• Core global backbone (e.g. fibre) which carries trans-continental internet traffic • Co-location facilities enabling network operators to interconnect with other operators		• Backbone ISP: AOL, Cogent • Backbone provider: AT&T, Global Crossing, FLAG Telecom, COLT • Co-location facilities: TELEHOUSE, RedBus, TeleCity
Content navigation	• Services which enable the user to search the internet for relevant content and applications	• Can filter search results according to user preferences • Can categorise websites to allow	• Google • Lycos • Digg

Value chain element	Core activities	Potential consumer protection roles	Example players
		users to restrict search to relevant categories of users only	
Content access	• Software applications and supporting hardware that provide an interface enabling an end user to use internet services	• Filtering applications which are installed on a computer and filter out certain websites, SPAM etc. • Anti-virus/spyware applications which restrict the installation and spread of viruses and spyware • Hardware and/or software based firewalls which prevent unauthorised access to a computer network and monitors messages entering and leaving, blocking those which don't meet necessary security criteria • Software patches disseminated by vendors to remedy vulnerabilities	• Email: Outlook • Internet browsing: Internet Explorer, FireFox • Filtering software: McAfee
End user	• Consumer of internet content, services and applications	• Educational initiatives (e.g. media literacy) which teach users how to protect themselves online • Responsibility by the user for the content and services they access and contribute to (e.g. lawfulness, chaperoning children)	• General public

Section 4

Protection of personal data

4.1 The huge growth in computing power witnessed over the last thirty years or so, together with the increasing use of automated data processing in all spheres of life, has increased concern about the protection of personal data. Digital technologies, as well as the rise of the internet and its growing use for a range of transactions involving disclosure and exchange of personal data, have increased consumers' fears over the protection of their data. The number of organisations and companies that hold personal data has grown substantially while the electronic format in which data is now held makes it easier for data to be retained and shared.

4.2 When considering the protection of personal information, the starting point for most analyses lies with rights to privacy. The right to privacy is a basic human right enshrined in the 1948 United Nation's Universal Declaration of Human Rights and the 1981 European Convention on Human Rights (Article 8). Since the 1970s, many developed countries have responded to concerns about privacy risks arising from the collection and use of personal data by relying on "fair information principles" to govern the appropriate use of personal data. For example, such principles were laid out in the 1981 European Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, following the development of the OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data in 1980.

4.3 According to these principles, personal data can be collected lawfully for specific and limited purposes only, and can be stored only for as long as necessary to fulfil the purpose. Data must be accurate and adequate for the intended purposes, and individuals have a right of access to and correction of their personal data. The Convention also established special protection for data of sensitive nature, such as, for example, data on the individual's religious and political beliefs or medical records. Many of these principles have been formally adopted through data protection legislation.

4.4 For the purposes of this report, we have identified three major consumer protection issues that relate to the potential misuse of personal data to engage in unlawful, fraudulent or unethical activity:

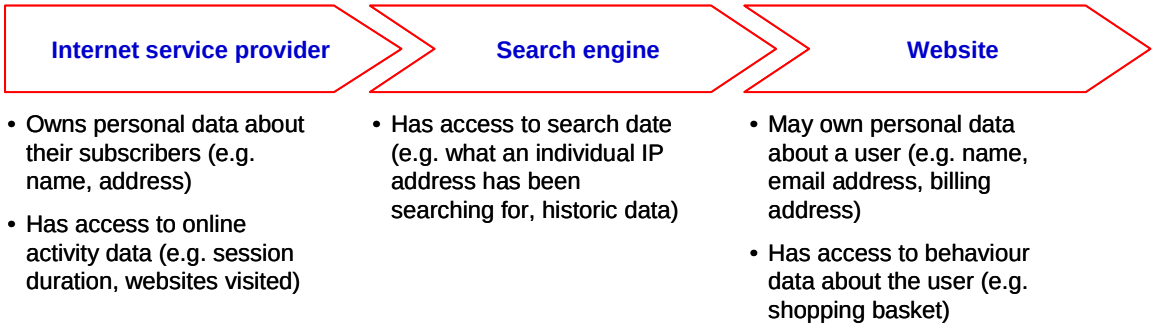
- Protection of personal data and monitoring of users' online activities
- Identity theft by phishing and pharming
- Unsolicited bulk email or SPAM.

4.5 It is important, however, to bear in mind that ways to misuse personal information are constantly evolving. One of the key challenges for government, regulators, enforcers and industry lies in responding swiftly and effectively to new forms of abuse.

Protection of personal data and monitoring of users' online activities

4.6 There are many ways in which an internet user provides personal data , as illustrated in one example below.

Figure 4.1: Data collection and retention across an example internet lifecycle



4.7 There has been increasing concern about how aware consumers actually are about the disclosure of their data online, especially when data is collected unknowingly. For example, a common method by which personal data can be collected from an individual without their knowledge is through the use of 'spyware' - software installed on an individual's computer which covertly transmits information about the user's activities to a remote host.

4.8 There is no conclusive definition of the term spyware, although for the purposes of this report we define spyware as comprising of two types: 'malware' and 'adware'. Malware includes viruses, worms and trojans and its defining characteristic is that it is intended to cause harm to the computer or be otherwise used for criminal purposes. We discuss malware in Section 7 of the report.

4.9 Adware is distinct from malware in that it does not have a malicious intent, but rather is designed to enhance the effectiveness of advertising targeted at the user or otherwise provide marketing information to a third party. Examples of this are applications that facilitate pop-up browser windows, redirect browser home pages and add favourite sites to browser lists. In addition, data tags referred to as cookies can be used by websites to identify users. On their first visit to a specific website, users may have a cookie downloaded onto their computer, which allows the website to recognise that user and their preferences when they return.

4.10 However, in the majority of cases users are not aware a) what spyware is and b) that it has been installed on their computer, creating potential privacy issues as personal data about them is being collected and distributed without their knowledge.

International framework

4.11 The growth of the internet has exacerbated many issues concerning the protection of personal data, particularly across national borders. In response, the EU and APEC (Asia Pacific Economic Cooperation) have developed agreements to harmonise their Members' approach to legislation regarding internet data protection. Of the international organisations developing data protection laws relating to the internet, the EU has been the most active, developing both legislative instruments and guidance that aim to protect data and underpin the free flow of goods and services within the EU.

4.12 There are three EU directives that relate to the protection of personal data. The first is the Directive of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data. The 1995 Directive lays out six conditions of legitimate date processing one which is unambiguous consent before data may be collected, with limited exceptional cases, for example, if it is in the vital interests of the subject, to ensure legal compliance, or

in the interests of national security. The 1995 Directive prohibits the collection of specific types of data (e.g. race, ethnicity, religious beliefs, political opinions, health), unless under exceptional circumstances, and requires those collecting, processing and retaining data to institute technical and organisational security measures to protect the data.

4.13 The second is the Directive 97/66/EC of 15/12/1997 Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector. The 1997 Directive aims to harmonise and provide an equivalent level of privacy and data protection as provided by the 1995 Directive but specifically within the telecommunications environment. It includes responsibilities on telecoms providers to maintain security of the network and traffic/billing data, and the right of individuals not to appear in publicised directories.

4.14 The third is the Directive of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector. The 2002 Directive updates and replaces the 1997 Directive (97/66/EC) and deals specifically with internet related issues. It includes the legal protection of new internet data, such as traffic data (e.g. routing information, session duration) and focuses on the confidentiality of electronic communications, data retention of users' online activities, spamming and inclusion of personal data in public directories.

4.15 Other international agreements include the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28/01/1981. The 1981 Convention aims to strengthen the legal protection of individuals with regard to automatic processing of personal information relating to them. It includes basic provisions requiring the lawful collection of data, secure and confidential retention of data, maintenance of accurate data and the right to access data by the subject, effectively harmonising signing Member States' legislation. It also includes provisions on the cross-border flow of data and international collaboration in the implementation of the treaty. The convention has been ratified by 35 Council of Europe Member States.

4.16 The OECD Guidelines, referred to earlier, have been signed by 30 OECD Member States. They set out data protection and privacy principles to be observed by signing States, including limits on how personal data is collected and used and requirements on signatories to secure information flows across borders and cooperate in areas related to data protection. The OECD continues to be active in this field, especially through the work of its Working Party on Information Security and Privacy.

4.17 Finally, the Asian-Pacific Economic Cooperation (APEC) Privacy Framework promotes a consistent approach to information privacy protection across APEC member economies, including the development of appropriate privacy protections for personal information, and the prevention of unnecessary barriers to information flows.

UK regulatory approach

4.18 Data protection has become increasingly important in the UK. The measures employed in the UK in order to protect individuals' right to privacy and ensure protection of personal data include both direct regulation and self-regulatory measures.

4.19 Along with other Member States of the European Union, UK has implemented the 1995 Directive (95/46/EC) of the European Parliament on the Protection of

Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data through the 1998 Data Protection Act (DPA).

4.20 The Data Protection Act came into force in 2001. It was amended by the Freedom of Information Act of 2000 to cover additional issues in relation to public authorities, including colleges and universities. The DPA places obligations on those who process information ("data controllers") and gives rights to those who are the subject of that data ("data subjects", such as consumers). The body responsible for ensuring compliance with the DPA is the Information Commissioner's Office (ICO) which is an independent regulatory authority. All organisations processing personal information must notify the Information Commissioner's Office of their activities, unless they hold an exemption under the Act.

4.21 DPA requires all those processing personal information to comply with enforceable principles of good information handling practice which require personal data to be collected fairly and lawfully, kept accurately and retained for no longer than necessary. The Act also requires specific measures to be put in place to limit unauthorised access to and processing of personal data. It provides data subjects, for example, with rights to access their data, to prevent data being processed where it may result in damage or distress, and to receive compensation in the event of breaches of the Act. The DPA also requires that personal data not be transferred to countries outside European Economic Area unless those countries have adequate protection for the individual.

4.22 Another element of the direct legislation dealing with the issue of personal data are the Privacy and Electronic Communications (EC Directive) Regulations of 2003. These regulations implement the EU Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector into UK law. The Regulations cover unsolicited direct marketing communications by email or SMS. The Regulations came into force in 2003 and are enforced by the Information Commissioner's Office.

4.23 There are two key areas where the 2003 Regulations have applicability to the internet:

- The use of cookies on websites
- Direct marketing practices.

4.24 The 2003 Regulations introduce strict restrictions on the use of cookies on websites. The use of cookies requires websites to give users clear and comprehensive information about the purpose of cookies, to enable users to give consent to the use of cookies or to refuse them. If cookies contain personal data, websites must also comply with the Data Protection Act.

4.25 With respect to online direct marketing practices, the Regulations require all campaigns to obtain customers' consent to receive marketing communications. If the campaign is run under an existing customer relationship, direct marketers have to provide users with an opt-out mechanism only, that is, an option to stop receiving marketing communications.

4.26 In addition to the direct regulation, many industry associations have established their own self-regulatory measures in the form of Codes of Conduct that their members are expected to adhere to. The codes are designed to provide guidance to companies on how to comply with personal data protection legislation, as well as to

encourage end users to attempt to take all possible precautions to protect their personal information.

4.27 Examples of such self-regulatory measures include the internet Services Providers' Association (ISPA) Code of Practice, which requires members to comply with UK law regarding data protection and privacy, and the TrustUK seal programme, which can be used by online traders to indicate to their customers that they adhere to strict privacy policy and provide a safe online environment. TrustUK seal programme currently has 9,000 members.

4.28 Data protection issues, however, remain live. The Information Commissioner's Office received over 19,000 complaints from the general public in 2004[19].

4.29 The UK regulatory environment relating to the use of consumer data obtained through the use of spyware, such as adware, is still at an early stage of development but is moving towards a self-regulatory framework.

4.30 There is currently no UK legislation which focuses specifically on the use of adware. However, in June 2004, the All Party Internet Group (APIG), a discussion forum for parliamentary members and industry that acts to inform parliamentary debate, recommended that cases of the misuse of adware could be dealt with under existing Data Protection Act legislation. The Data Protection Act suggests that adware is legal in the UK, as long as it was installed on the computer with the user's explicit consent.

4.31 In addition, the Privacy and Electronic Communications Regulations specifically cite covert use of 'cookies' or other monitoring devices as illegal and empower the Information Commissioner's Office to enforce such infringements.

4.32 However, the definition of covert use of adware is not clear-cut as adware applications are often provided as part of a bundle of software and, therefore, users may not be aware of exactly what they are downloading as part of the software package. To this end, the APIG has recommended a self-regulatory environment, with the development of Codes of Conduct by the software applications industry which would include provisions regarding clarity of terms at the point of installation. To date, there has not been any concerted effort by industry to address this issue. This makes widespread awareness of the availability of firewalls, and the supply of affordable and easy-to-use firewalls, even more important.

International approaches

4.33 Like the UK, most EU Member States have translated EU Directives discussed above into national law and have established independent regulatory authorities tasked with enforcing personal data protection. Representatives from the national regulatory authorities also work at EU level, through their membership of the Article 29 Data Protection Working Party.

4.34 Additionally, self-regulatory models have evolved in many EU countries. For example, Internet Service Providers Associations in Austria and Ireland (ISPAI in Ireland and ISPA in Austria) have established codes of conduct which include provisions on data protection.

[19] Information Commissioner's Office, Annual Report 2004/05

4.35 The combination of direct legislation and self-regulatory approaches also extends to non-European countries, such as Canada and Hong Kong. In Canada, the Office of the Privacy Commissioner is a direct regulatory body which enforces privacy and data protection legislation. The Office is complemented by industry self regulation through the Canadian Standards Association Model Code for Protection of Personal Information, a model code developed by the Canadian Standards Association (CSA). The internet industry body, the Canadian Advanced Technology Alliance (CATAAlliance) has recommended the use of this code to its members.

4.36 Hong Kong also uses a hybrid of direct and self regulation. It regulatory body, The Office of the Privacy Commissioner for Personal Data enforces legislation, whilst industry bodies such as the Hong Kong Internet Service Providers Association have developed their own self regulatory codes of conduct with provisions on data protection.

4.37 There are, however, different models for tackling the issues of personal data protection. In this report, we will highlight two examples of divergent regulatory approaches – the co-regulatory model found in Australia, and the self-regulatory model found in the USA.

Case study - Australia

4.38 The core of the Australian model is the 1988 Privacy Act which includes eleven Information Privacy Principles which must be complied with by government agencies and organisations. The Act was amended in 2001 and 2002 to extend to healthcare providers and certain areas of the private sector.

4.39 Under the Act, the Office of the Privacy Commissioner, an independent regulatory authority, is responsible for enforcing the codes where necessary. However, the Act also stipulates that industry organisations can develop their own Codes of Conduct. The Codes must be ratified by the Office of the Privacy Commissioner, but once ratified, they replace the Act as binding regulation. In such cases, the associated industry organisations replace the function of the Office of the Privacy Commissioner and become responsible for the enforcement of the code.

4.40 A number of industry organisations have already adopted this approach, such as, for example, the Association of Market Research Organisations, the Insurance Council of Australia and the Queensland Clubs. Several other industry organisations are now looking to do the same, including the Internet Industry Association which has submitted a draft code of conduct which would apply to all Australian internet content providers, hosts and service providers.

Case study – the USA

4.41 The United States, on the other hand, so far has adopted a predominantly self-regulatory model, with exceptions in specific areas. The existing direct legislation in the USA that deals with the issue of data protection has a limited reach. The 1974 Privacy Act covers the transfer of personal data between government agencies and departments. There are three further areas where data protection is granted through direct regulation:

- Financial and healthcare services are regulated by sector specific privacy acts, for example the Gramm-Leach Bliley Act and the Fair Credit Reporting Act for the financial sector

- The protection of data from unauthorised access is provided in some states through security breach notification legislation, such as California's 2003 Security Breach Notification Act

- Data protection in relation to minors is provided through the Children's Online Privacy Protection Act

4.42 The regulatory body responsible for the enforcement of specific data protection laws is the Federal Trade Commission (FTC).

4.43 With the exception of specific areas covered by the law, data protection follows a self-regulatory approach. The FTC encourages the industry and individual companies to develop and publicise self-regulatory codes of conduct and privacy policies. The FTC is empowered to investigate and issue fines for breaches in company privacy policy, but only where the company has explicitly broken its published policy.

4.44 In response to the calls by the FTC, some self-regulatory initiatives have been established in the USA. A notable example is the Better Business Bureau (BBB) privacy seal, which uses a graphical logo to indicate the website's compliance with the BBB's online privacy code of conduct.

4.45 The lack of over-arching data protection legislation in the USA covering both commercial and public sector organisations had international ramifications. The European data protection directives prohibit the transfer of personal data to countries without 'adequate protection' and until July 2000, the US was included on the banned list. However, following the approval of the 'Safe Harbor Initiative' by the EU in July 2000, the USA has been removed from the banned list. The Safe Harbour Initiative now provides one means for US companies dealing with EU data to comply with the EU data protection regulations.

Case study – the USA

4.46 In relation to adware, very few countries have developed regulatory measures that deal specifically with the issue of adware. A notable exception is the USA which has opted for both direct legislation and self-regulatory initiatives.

4.47 The US federal government has recently passed four bills which focus specifically on the use of spyware:

- Securely Protect Yourself Against Cyber Trespass Act, 2004 - prohibits the use of computer software to collect personal information and to monitor the behaviour of computer users without consent

- Internet Spyware Prevention Act, 2004 - amends the Federal criminal code to prohibit intentionally accessing a protected computer without authorisation

- Software Principles Yielding Better Levels of Consumer Knowledge Act (SPY BLOCK Act), 2004 - makes it unlawful for an unauthorised person to install on a protected computer any software that collects information about the user's internet browsing or other activity, and transmits such information to another person.

4.48 As in other cases, the FTC is the regulatory authority empowered to enforce the laws and issue fines in instances of violation. The FTC has also actively encouraged further self-regulatory initiatives. The Direct Marketing Association has established a

code of practice which applies to cookies and adware used by its members, while the Web Analytics Association (which conduct online consumer analysis) has released a Statement of Principles with respect to spyware which is yet to be ratified.

Conclusion

4.49 A combination of direct regulation and self-regulatory initiatives has been used in many developed countries to address concerns about the protection of personal data. Legislation, when appropriately enforced, can create a powerful deterrent to potential infringers of the law. However, the use of complementary self-regulatory tools can allow the industry to develop and implement its own solutions in ways which can provide additional confidence to consumers.

4.50 While self-regulation engages the industry in developing own practical solutions, the US model, which relies primarily on self-regulation, illustrates its potential downside. The model relies on websites being pro-active in taking steps to protect their users. However, as there are no mandatory obligations in place and no means of enforcement, many websites have failed to take such action, leaving US consumers potentially at risk in relation to protection of their personal data.

Identity theft by phishing and pharming

4.51 Identity theft refers to the unauthorised use of an individual's personal information in order to commit fraud or other crime.

4.52 There are two key points at which personal information can be stolen:

- From the organisation holding the consumer's information); or
- Directly from consumers themselves.

4.53 The former is usually the result of security breaches in the company's network. Such breaches can have important and material impact on the consumers, and companies are responsible for ensuring their systems offer adequate protection to their customers. In this report, we will not discuss issues relating to security breaches of corporate or public organisations.

4.54 The online fraudulent theft of personal information directly from the consumer is often referred to as 'phishing' and at present can be accomplished in a variety of ways, including:

- Deceptive phishing
  - The consumer target receives a deceptive email, for example, a fraudulent notice of an undesirable change being made to their account, which prompts the consumer to connect to a website
  - The website to which the consumer is normally directed resembles that of a bona-fida organisation, for example the consumer's bank, and will require users to input their confidential details which are then collected by the phisher
  - In some cases, consumers are asked for their confidential details to be sent back by email, eliminating the need to activate the web browser
- Malware-based phishing

- The consumer target's machine is infected with malicious software, employing different methods to collect the user's information.

- Malware-based phishing is manifested in one of three ways:

1) Through constant monitoring of the user's machine by means of software which monitors data inputted by the user and sends the data to the phisher

2) Through the remote hijacking of sessions which activate once a user has legitimately established their credentials

3) Through web trojans which pop up over login screens and appear to be genuine login websites

- DNS-based phishing

  - This interferes with the integrity of the lookup process when transferring from a domain name to an IP address

- Content injection phishing

  - Malicious content is inserted onto a legitimate site

- Search engine phishing

  - Phishers create web pages for fake products, often 'too-good-to-be-true' products, which are then indexed by search engines.

International framework

4.55 At an international level, there has been a growing recognition of the need for individual nations to recognise the misuse of personal data and identity theft as a crime, and cooperate effectively to investigate, capture and prosecute perpetrators of such crime. In response, a number of international agreements have been made recently to facilitate cooperation in tackling the issue of identity theft.

4.56 Council of Europe Convention on Cybercrime, Budapest 23/11/2001 was the first international treaty addressing cyber crime. Signatories to the Convention are required to enact national laws criminalising four categories of computer related crime:

- Fraud and forgery

- Child pornography

- Copyright infringements

- Security breaches such as hacking, illegal data interception, and system interferences that compromise network integrity and availability.

4.57 The Convention requires signatories to establish a process for detecting, investigating, and prosecuting defined cyber crimes. It calls for measures to retain data and electronic communications and allow real-time data interception, but also recognises that signatories must safeguard the protection of human rights. The Convention also establishes a system for international cooperation including a 24-

hour, seven-days-a-week contact network to provide immediate assistance with cross-border investigations. So far, there have been 30 signatory countries (including Canada, Japan, South Africa and the US) and 12 ratifications.

4.58 APEC Cybersecurity Strategy, formed in October 2002, contains a non-enforceable recommendation to member states to adopt legislation and policies criminalising cybercrime, establish hi-tech crime units with 24/7 points of contact and share information about cybersecurity best practice.

4.59 EU Council Framework Decision 2005/222/JHA of 24 February 2005 on Attacks Against Information Systems criminalises illegal access to information systems and illegal system and data interference, and sets out sanctions for perpetrators of such activities. In addition to identity theft, the Framework Decision covers a range of cybercrimes including hacking, "denial of service" attacks, and spreading of computer viruses. The Framework Decision is also "technology neutral" and counts all devices connected to networks, including mobile phone and PDAs, as relevant "Information Systems". The deadline for implementation of the Framework Decision into national law is 16 March 2007. As a Member State, the UK will also have to implement it.

4.60 The European Commission has also taken further steps to encourage the development of a secure information society. In 2004, it created the European Network and Information Security Agency (ENISA) whose main tasks include:

- Collecting and analysing data on emerging security issues in Europe
- Advising the Commission and the Member States on information security and security-related problems in hardware and software
- Promoting risk assessment and management methods
- Raising awareness and co-operation among different actors in the information security field, and encouraging development of public / private partnerships.

4.61 The Antiphishing Working Group (APWG) is an example of an international self-regulatory initiative to tackling phishing. APWG is a not-for-profit industry association whose members include financial institutions, online retailers, ISPs, the law enforcement community, security solutions providers and research institutions. This group provides a forum for sharing best practice for tackling phishing attacks. Victims of online identity theft can also report instances of attack to the APWG, although AWPG states clearly on its website that, due to the volume of such attacks and the voluntary nature of the organisation, it may not be able to deal with reports quickly.

UK regulatory approach

4.62 Phishing incidents are becoming increasingly common. The Get Safe Online campaign, sponsored by the UK government and industry, estimated the total cost of phishing in the UK in 2005 to have reached £12m[20]. The cost of online identity theft and phishing is still a relatively small proportion of the total cost of identity fraud, estimated to cost the UK more than £1.3bn each year [21]. Likewise, the consumer fear of internet crimes such as phishing is still substantially lower when compared to

[20] Get Safe Online
[21] Association for Payment Clearing Services (APACS)

that of offline crimes - 17% of consumers rate internet crime as their biggest crime fear compared to 40% who rate bank card fraud[22].

4.63 However, phishing attacks are on the increase in the UK. Globally, the Anti Phishing Working Group reported 16,882 unique attacks in November 2005, up from 8,975 unique attacks launched in November 2004[23].

4.64 Phishing and online identity theft are instances of deception under current UK Theft Acts (1968-1996) and, as such, it is the role of the police to investigate reports from victims of such activity. However, the way that the criminal law dealt with fraud had long been considered vague and confusing by the law enforcement agencies. The 2002 Law Commission report on fraud recommended a reform of the criminal law to make it easier for instances of fraud to be identified and for perpetrators to be prosecuted effectively.

4.65 As a result, the Government has proposed a new bill, the Fraud Bill, which introduces a general fraud offence in order to strengthen existing laws, especially with respect to fraud offences committed online. The new fraud offence can be committed in one of three ways:

- By false representation (as in the case of a phishing attacks)
- By failing to disclose information
- By abusing a position of trust.

4.66 The Fraud Bill also introduces a new offence for obtaining services dishonestly and participating in a fraudulent business, such as, for example, making fraudulent credit card transactions online. The Fraud Bill makes it an offence to possess, manufacture or supply any equipment which facilitates fraud, including for example, computer malware designed to collect users' financial data.

4.67 Importantly, under the proposed new law, fraudsters posing as financial institutions in phishing attacks could become the subject of extradition proceedings. The Fraud Bill was introduced in May 2005 and is currently with the House of Lords. It is expected to become law in 2006.

4.68 The rapid rise of instances of identity theft has prompted further measures by the Government. The Home Office has recently set up the Home Office Identity Fraud Steering Committee. This is an initiative launched in collaboration with other government departments and private sector organisations, and its aim is to facilitate cross public/private sector work programme tackling identity theft and identity fraud. The Committee has set up the Identity theft website (www.identity-theft.org.uk) which provides consumers with information on how to protect themselves and where to seek help should they become a victim of identity theft. Additionally, the Government has established specific police units with expertise in investigating internet-related crime, such as the National Hi-tech Crimes Unit, which started in 2001.

4.69 Under the current regulatory regime, sites hosted from the UK which perpetrate identity theft are investigated by the police, with cooperation from relevant ISPs.

[22] Get Safe Online
[23] Anti-Phishing Working Group Phishing Activity Trends Report, November 2005

There are, however, no industry wide Codes of Conduct which govern the cooperation between the police and the ISPs.

4.70 Since the primary target for identity theft crimes has been the financial services industry, the onus has been on the financial services providers to increase their security measures and warn their customers about the existence of risks around identity theft. As a result, various industry associations have taken a pro-active role in sharing best practice and information regarding the dangers of identity theft. An overview of the role of some financial institutions in tackling identity theft is outlined below[24]:

- Financial Services Authority (FSA)
    - The FSA has implemented a customer education initiative to raise awareness about the issues of online identity theft, as well as a process for dealing with reports of instances relating to identity theft. As part of the customer education initiative, the FSA provides best practice information to consumers on how to avoid being targeted
- British Bankers Association (BBA)
    - The BBA tries to raise awareness both amongst its members (i.e. the banks) and end users as to how to prevent and deal with online identity fraud. It provides best practice tips for the banking industry on preventing and responding to phishing attacks and produces consumer information concerning identify theft
- UK Payments Association (APACS)
    - Similar to the BBA, APACS provides best practice information to companies on how to secure against, and respond to, instances of online identify fraud and phishing
- Banksafeonline.org.uk
    - This is the UK banking industry's initiative to help banking users stay safe online. It provides consumers with information on how to spot online scams and what measures to take to protect themselves.

4.71 By its very nature, fraud is fast-changing, often international in nature, and in many instances subject to the involvement of organised crime. This makes it a particularly difficult issue to address. While the issue of identity fraud has moved up the political agenda, the debate continues about how best to tackle fraud, especially fraud which uses the financial services sector. Going forward, and more than ever before, it will be essential that government, regulators, enforcers and industry work closely together, in order to minimise the harm that can be caused to consumers.

[24] See the FSA's report "Developing our policy on fraud and dishonesty" (http://www.fsa.gov.uk/pubs/discussion/dp26.pdf) for more information on the organisations involved in tackling fraud within the financial services sector.

International regulatory approaches

4.72 Like UK, most countries around the world are experiencing an increase in the incidence of online identity theft and, as a result, are developing measures to educate consumers about the dangers they could encounter online, and improve online transaction security. And like in the UK, many of these measures are self-regulatory initiatives led by the industry.

Case study – the USA

4.73 The US has adopted a self-regulatory model for tackling online identity theft, with a particular focus on the financial services industry. The Federal Financial Institution Examination Council (FFIEC), a governmental agency empowered to recommend and prescribe uniform principles and standards to financial institutions in the United States, published a recommendation in October 2005 titled the Authentication in an Internet Banking Environment. The recommendation is aimed at the US banking industry and calls on financial institutions to adhere to the specific guidelines in order to safeguard customer information, such as, for example, using multifaceted factor authentication, layered security and other controls.

4.74 There are also two important industry-led measures that have been taken at an international level:

- Data encryption through the https security layer in the http protocol
- Data encryption through a digital signature

4.75 https is an additional security layer in the http protocol and is widely used on commercial websites. It was originally developed by Netscape Communications Corporation, but certificates for its use are now built into the majority of internet browsers.

4.76 https encrypts data which is inputted during a user's online session, ensuring a secure channel between the user's browser and the web server. The user is able to recognise the use of this additional security layer in two ways - a) the web page address will alter from http://www. to https://www, and b) a padlock symbol will be displayed on the user's computer screen (usually in the bottom right hand corner). Essentially, this aims to ensure that all data transmitted using https is secure and cannot be tampered with by a third party.

4.77 https has been widely adopted by online banking and commercial sites in order to secure the link between the user inputting their financial details – for an online bank this may be a password, for a commercial site this may be credit card details. This system also aims to give a peace of mind to the user that their internet transactions are being carried out through secure channels.

4.78 Digital signatures are another encryption method used to securely transmit data, though they are usually associated with the corporate environment. These signatures use Public Key Infrastructure (PKI), a system which allocates a private key to the user which encrypts the data to be sent with a personalised data signature. The data receiver holds a public key, which decrypts the data and authenticates that it was sent from that user.

Conclusion

4.79 There are three key challenges to tackling the issue of phishing. The first challenge is that of detection - phishing relies on employing highly sophisticated technology to deceive consumers without being detected and therefore, in most instances, a phishing incident is not reported until the damage has already been done (e.g. the money has already been taken from the consumer's account).

4.80 The second challenge comes from the international nature of the internet. Phishers often operate on a global scale, making the investigation and capture of the perpetrators inherently difficult as it is dependent on the harmonious national laws and the effective cooperation between different national internet crime units. Therefore, gaps and differences in the laws of the different countries may hamper the fight against trans-national cyber crime and may complicate efficient law enforcement.

4.81 Finally, the short time period over which phishing attacks occur makes capture very difficult. On average, phishing sites are only operational for 5.5 days before closing down, and the greatest financial damage takes place in the first few hours of the operation. Due to delays in detection by consumers, the time window for enforcement agencies to investigate and detain perpetrators is usually very short.

Unsolicited bulk email or SPAM

4.82 SPAM is the name given to unsolicited and unwanted emails messages. It is the online equivalent to junk mail, but unfortunately takes place on a much larger scale. It is estimated that over 85% of all email traffic is SPAM, putting unnecessary traffic pressure on networks and clogging up a user's email inbox[25].

4.83 SPAM is irritating for users and expensive for network operators. It can also have more serious consequences for the consumer - although a substantial portion of SPAM is just advertising, some SPAM emails contain viruses or spyware which will be installed on the user's computer once opened. SPAM emails can be used as a mechanism for fraudulent activities advertising fake products, get-rich-quick schemes and other scams. SPAM email messages can also be used for phishing attacks attempting to deceive a consumer into releasing their financial details.

4.84 SPAM has become a high profile issue on an international level. International organisations such as the Organisation for Economic Cooperation and Development (OECD) and International Telecommunications Union (ITU) have both focused on SPAM in their recent work. In 2005, both organisations published in-depth reports on different approaches to tackling SPAM and organised events to facilitate international cooperation on the issue. Additionally, the OECD has produced an anti-SPAM toolkit aimed at educating governments, regulators, industry members and consumers on different approaches to tackling SPAM. It is available at www.oecd-antispam.org.

4.85 In response to a recognition that SPAM is an international issue with international ramifications, a number of multinational agreements have been reached to facilitate sharing of best practice approaches to tackling SPAM and ensure cooperation across national borders.

[25] Messaging Anti-Abuse Working Group Q4 2005 Report

4.86 The London Action Plan was signed in October 2004 as an inter-governmental agreement between 15 different countries and a number of private sector companies, including ISPA UK. The London Action Plan agrees effective communication and coordination between national agencies to achieve efficient cross-border enforcement of anti-spam laws, increased collaboration on effective ways to bring SPAM cases against bulk mailers, and an exchange of information and best practices.

4.87 The APEC Recommendation on Combating SPAM was issued in June 2005, following a ministerial meeting. It includes implementation guidelines to members' economies on anti-SPAM strategies. The guidelines are intended for governments, industry and the general public.

4.88 The Declaration of 30/03/2005 of the Conférence des Administrations des Postes et des Télécommunications d'Expression Française (CAPTEF) was signed by 22 French speaking African countries. The Declaration recognises the importance of the fight against SPAM and requires signatories to appoint national contacts responsible for targeting SPAM. The national contacts are in turn responsible for reporting SPAM to international organisations such as OECD and ITU. The Declaration also emphasises the need for cooperation and knowledge sharing.

4.89 Asia-Europe Conference (ASEM) issued a Joint Statement on Anti-spam Cooperation in February 2005, following its e-commerce conference in London. The signatories include 25 European and 13 Asian member states. They have agreed to take action to fight SPAM nationally and to promote anti-SPAM efforts in international organisations as well as by the industry.

4.90 In addition to formal agreements, there have been several multinational educational campaigns to drive awareness on SPAM. A recent, high profile example is Operation SPAM Zombies, a US Federal Trade Commission-led campaign which is working with 35 government partners to educate ISPs and other internet connectivity providers about hijacked, or "zombie" computers that spammers use to flood in-boxes.

UK regulatory approach

4.91 SPAM is a significant problem in the UK, with the amount of SPAM increasing by 13% in 2006. It is now estimated to account for around 85% of all email traffic. In a recent AOL Consumer survey, the number one annoyance for internet users was SPAM, making it an important consumer issue in the UK.

4.92 The main regulatory tool in the UK for dealing with SPAM are the Privacy and Electronic Communications Regulations (PECR) discussed above. The Regulations prohibit the sending of SPAM where the receiver has not consented to receive it, that is, the Regulations set out an opt-in approach for SPAM. Additionally, the Regulations require all electronic mail senders, including bulk mail senders, to identify themselves to consumers and to provide an option to opt-out of receiving further mails in every communication sent to the consumer.

4.93 The Information Commissioner's Office (ICO) is the independent regulatory authority responsible for dealing with complaints relating to SPAM and taking enforcement action against perpetrators. If an enforcement notice issued by the ICO is breached, the ICO can prosecute the offender.

4.94 The current UK regulatory approach targets the senders of SPAM and does not place any specific obligations on ISPs other than to comply with the relevant authorities in locating individual perpetrators. However, as in many other countries, the actions taken by the ISPs have been most the effective tool in reducing the impact of SPAM on the consumer. All major UK ISPs now offer SPAM blocking services as part of the standard subscription package and the ISP industry association, ISPA, encourages its members to provide SPAM filters to subscribers. SPAM filters have proved a very useful measure against SPAM and their widespread adoption has been key to tackling the issue.

International regulatory approaches

4.95 In the majority of countries, the sending of unsolicited emails is illegal and the law is enforced either through specially established branches of the police or through statutory authorities. Anti-spam legislation has been introduced in the USA, South Korea as well as in Member States of the European Union. However, the nature of the legislation varies. Like the UK, some countries criminalise the act of sending SPAM where users have not already explicitly 'opted in'. Other countries allow SPAM to be sent unsolicited so long as the sender provides the consumer with the option to 'opt out' of receiving further communication. Under the latter model, only SPAM sent to an 'opted out' address would be deemed illegal.

4.96 Across the European Union, legislation relating to SPAM has been harmonised via the European Directive on Privacy and Electronic Communications (2002/58/EC) which led to the Privacy and Electronic Communications Regulations (PECR) in the UK. This means that EU Members States have taken a similar approach to the UK of using direct regulation to establish an "opt-in" model for SPAM.

Case study – South Korea

4.97 South Korea is an interesting example of a different approach to using direct regulation to tackle the issue of SPAM. South Korea's system is based on an opt-out by the end user, rather than an opt-in as is the case in the UK.

4.98 Two statutes passed by the South Korean Government in 2001 and 2002 mandate that bulk messages can be sent as long as the receiver has not explicitly opted out from receiving such mail. All bulk messages must contain the identity of the sender and an explicit option to the receiver to opt-out of receiving such messages in the future. Collecting email addresses via technical means, and sharing and exchanging address lists, or participating in computer-generated addresses (e.g. 'dictionary attacks') is prohibited.

4.99 Additionally, the statutes mandate a 'subject-labelling' scheme for email SPAM: for example, email SPAM containing commercial messages must contain 'ADV' in the email subject header while email SPAM containing adult messages must contain 'ADLT' in the email subject header. The statutes contain provisions which allow ISPs and web mail providers to deny services to senders if they have reasonable suspicions that provision of the service is giving rise to SPAM.

4.100 The regulations are enforced by the Korean Spam Response Centre, a central agency tasked with investigating complaints made by receivers of SPAM. The Korean government has embarked on programme to educate consumers about SPAM and is using an online campaign to distribute free SPAM filter software.

Conclusion

4.101 Anti-SPAM legislation has already been used to prosecute offenders and deter potential spammers. In the US, the anti-SPAM legislation, the Can-Spam Act, was recently used by AOL US to bring a civil law suit against an individual who sent billions of junk e-mails offering online college degrees and links to sexually explicit websites. The US Federal Court upheld the complaint and ordered the defendant to pay more than $5 million in penalties. This strict ruling was seen as a success by the ISP industry in sending a strong message to spammers that illegal activities would not be tolerated.

4.102 However, the volume of SPAM traffic is still extremely high. It generates a significant cost to the industry which may in the end be passed on to the customer. Many UK ISPs are currently calling for harsher penalties and punishments to deter spammers from continuing their activities. However, the international nature of SPAM presents significant constraints on any action to eliminate SPAM – the great majority of cases of SPAM involves senders operating from a different country to that of the recipients.

Section 5

E-commerce

5.1 In recent years the internet has become an established mechanism for trade, with the total UK e-commerce market reaching £8.2bn in 2005, representing a 29% increase on the previous year[26]. During the 2005 Christmas period, UK shoppers spent nearly £5bn online[27].

5.2 There is, however, evidence to suggest that consumers still perceive the online commerce world to be less safe than the offline world. Many consumers have concerns about inaccurate descriptions of goods, lack of returns policy or warranty for faulty products, and non-delivery of goods. They are also concerned about the incidence of fraud using the internet; while 54% of internet users are happy to enter personal email address on the internet, only 28% of users say they are likely to disclose credit card information on the internet[28]. Building enduring consumer confidence in the internet as a commercial transaction medium will, therefore, be a key challenge in taking full advantage of the opportunities created by a global marketplace.

Consumer protection regulation with respect to trading standards

Introduction

5.3 Trading standards regulation has a long history in the offline world and consumer protection from poor business practices has long been embodied in law. In the UK, the Sale of Goods Act 1979 (amended by the Sale & Supply of Goods Act 1994 and the Sale and Supply of Goods to Consumers Regulations 2002) ensures that whenever consumers purchase goods from a trader, they automatically receive certain statutory rights under the Act.

5.4 For example, consumers have a right to goods that are:

- Of a satisfactory quality, i.e. generally free from fault or defect, of a reasonable appearance and finish, and safe and durable.
- Fit for the purpose - goods should be fit for any specific or particular purpose made known at the time of the agreement.
- As described - goods should correspond with any description applied to them.

5.5 If the goods sold fail to meet these standards, the consumers are entitled to a refund, replacement or repair, subject to certain provisions.

5.6 However, available data suggests that many consumers still lack the confidence to extend their commercial activities into the online world despite the fact the internet has opened up a wealth of new opportunities for consumers. According to recent surveys, practically 90% of the e-commerce market still consists of business-to-

[26] Verdict market analysis
[27] Interactive Media in Retail Group (IMRG)
[28] Ofcom Media Literacy Audit 2006

business (B2B) transactions, and the development of the consumer market continues to lag behind[29].

5.7 A key reason behind consumers' lack of confidence is the perceived absence of consumer protection with respect to trading standards in the online world. Amongst the key issues that consumers are concerned about are payment security, product delivery, refunds and dispute resolution. A report produced by the European Consumer Centre Network, The European Online Marketplace: Consumer Complaints 2004, stated that 41% of all e-commerce related complaints concerned problems with product delivery, followed by 25% complaints related to product quality and conformity with the information provided to consumer. Such incidents tend to further damage consumer confidence[30].

5.8 Even though most analysts believe that growth is picking up - market growth in business-to-consumer (B2C) e-commerce is estimated at around 50% per annum, though it remains low in absolute terms[31] - the dominance of the market by B2B transactions suggests that the full potential of the market is not being realised for consumers.

International framework

5.9 At an international level, a substantial amount of work has been done to develop model legal frameworks governing the development of online trading market that nations can use as the foundations for their own national law. The creation of such common frameworks is seen as key to a successful and legitimate cross-border e-commerce environment as it would encourage harmonisation of the legal frameworks used by different nations.

5.10 The key objective of establishing a specific legal framework is legitimisation of online commercial protections, including:

- An adaptation of existing laws to give transactions received by electronic means the same validity as those carried out on paper, and to enable a contract to be completed entirely electronically; and

- Establishment of liability for services in the online world (for example, does the liability lie with the service provider or the access provider).

5.11 The United Nations Commission on Trade Law (UNCITRAL) was the first major international body to produce a model legal framework in 1996, the Model Law on Electronic Commerce. This has subsequently formed the basis of many national legal frameworks, including those of the USA (Uniform Electronic Transactions Act 1999), Canada (Uniform Electronic Commerce Act 1999), France and Ireland.

5.12 The Organisation for Economic Cooperation and Development (OECD) has been a leader in this area, producing in 1999 extensive Guidelines for Consumer Protection in the Context of Electronic Commerce.

[29] European Commission Working Document: Consumer Confidence in E-Commerce, 2004
[30] European Consumer Centre Network: The European Online Marketplace: Consumer Complaints 2004 Report
[31] European Information Technology Observatory (EITO 2004) 2003-2007 estimates

5.13 The guidelines aim to extend the existing legal protection that is available to consumers in more traditional forms of commerce and encourage greater co-operation among governments, businesses and consumers. Their objective is to support the development of best practice in online commercial transactions through:

- Fair advertising and marketing practices;
- Clear information about the identity of the business and the goods or services it offers
- Transparency about the terms and conditions of any transaction and about the process for confirming transactions;
- Secure payment mechanisms and protection of personal data;
- Fair, timely and affordable dispute resolution and redress

5.14 Although the implementation of these guidelines in the form of legislation has not been widespread, they have been used by many countries as the basis of their best practice guidelines to the e-commerce industry.

5.15 The EU has also long been active in the area of trading standards. In 1997, it issued the Distance Selling Directive (97/7/EC) with the aim of extending to consumers purchasing goods or services through distance communication means the same level of protection as that governing transactions with traditional brick-and-mortar companies. For the purposes of the Directive, distance communication means include traditional catalogue sales as well as new means of distance communication such as teleshopping, mobile phone commerce (m-commerce), and commerce on the internet (e-commerce).

5.16 The intention behind the Directive was the minimum harmonisation of the laws, regulations and administrative provisions of Member States in respect of distance contracts. Whilst the Directive refers to a certain level of “legal protection”, it allows Member States to introduce more stringent provisions into their domestic legislation in order to provide a higher level of consumer protection than that referred to in the Directive. The legal protections guaranteed by the Directive to consumers throughout the EU when undertaking commercial transactions online include:

- A requirement on e-merchants to provide consumers with comprehensive product or service information before the purchase
- Consumer’s right to cancel the purchase within a minimum of 7 working days without giving any reason and without penalty
- The right to a refund within 30 days of cancellation of purchase
- Delivery of goods or services within 30 days of the day after the consumer placed the order
- Protection from unsolicited commercial communication
- Protection from fraudulent use of payment cards.

5.17 The Directive also makes explicit the non-validity of any waiver of the rights and obligations provided for under the Directive, whether the waiver is instigated by the

consumer or the supplier. The provisions of the Directive are comprehensive and go much further than is the case in many non-EU countries where equivalent protection is recommended as best practice, but is not required by law[32].

5.18 The European Union has produced additional legislation with the aim of establishing an appropriate legal framework for e-commerce. Its 2000 Electronic Commerce Directive (2000/31/EC) establishes the country of origin principle, that is, the application of the jurisdiction of the country of the e-merchant's origin in disputes. Additionally, the Directive also establishes the freedom for internet services to be provided across borders, and the protection of service providers from forced closure from authorities outside of its home market. The Directive outlines basic trading obligations for the service provider to adhere to, such as minimal information requirements and contractual information. The Directive has been translated into national law by several Member States, including the UK.

5.19 The enforcement of consumer protection legislation has been challenging, especially in cases of cross border transactions. As a result, in 2004 the EU adopted legislation on enforcement cooperation among different national authorities, the Regulation on Consumer Protection Cooperation.

5.20 In addition, in order to foster the growth of safe cross-border commercial transactions, the European Commission has set up a number of consumer assistance networks. The European Consumer Centres and the European Extra-Judicial network provide consumers with assistance for out-of-court resolution of complaints and settlement of disputes especially across national boarders. Fin-Net focuses on assisting consumers with complaints regarding financial services across the EU.

5.21 Until recently, there has been a lack of formal agreements regarding cooperation between the European and other international agencies in addressing consumer complaints. Most of the work done at international level had been in the area of knowledge sharing. International Consumer Protection and Enforcement Network (ICPEN) was launched in 1992 as a major inter-governmental initiative dealing with consumer fraud and infringements of trading regulations. ICPEN has 33 national members, as well as the OECD and the European Commission, all of whom agree to a Memorandum of Understanding which mandates them to:

- Establish and maintain an up-to-date list of relevant enforcement contacts
- Attend annual conferences to exchange views and opinions on relevant topics
- Mutually exchange information to enable participating organisations to build up a picture of each other's methods and legal and administrative arrangements
- Co-operate informally at an operating level in preventing marketing malpractices as they arise.

5.22 ICPEN has recently taken steps to formalise international cooperation in enforcing of trading regulations. A new initiative, the econsumer.gov project, is a joint project of consumer protection agencies of member states of ICPEN whose objective is to offer

[32] Some types of contracts are excluded from all the provisions of the Directive. The exemptions include contracts for financial services and contracts concluded through an auction. Contracts for financial services are covered by the Distance Marketing of Financial Services Directive 2002/65/EC.

tools and information to enable consumers to make safe e-commerce transactions and enable consumers to register cross-border complaints. Complaints filed by consumers are maintained on the internet Sentinal, a US database accessible by all ICPEN member authorities.

5.23 While filing a complaint through the econsumer.gov initiative does not guarantee that it will be investigated by the relevant authority (the authority from the country where the infringer is based), the system provides a mechanism for identifying a greater number of rogue traders and taking actions against them.

5.24 Various international industry and consumer organisations are also working to raise the profile of online consumer protection. Examples of these include:

- Consumers International and the Trans-Atlantic Consumer Dialogue – umbrella organisation comprised of national consumer organisations, working at a international and transnational level respectively

- International Chamber of Commerce – an international industry association which lobbies on behalf of businesses and promotes best practice for online traders.

UK regulatory approach

5.25 The UK regulatory system for protecting the consumer in the online environment includes both direct and self-regulation. In the UK, general consumer protection legislation applies equally to the online environment. This legislation includes those measures regulating misleading advertising, false trade descriptions, misleading price indications, and provision of consumer credit. However, the growth of online transactions and the impersonal and borderless nature of the internet has called for additional legal measures to be taken to ensure consumers are adequately protected in their online transactions.

5.26 The UK legislative framework governing consumer protection in the online world is largely based on various EU Directives. The four main legislative tools in this area include:

- Consumer Protection (Distance Selling) Regulations 2000

- Electronic Commerce (EC Directive) Regulations 2002

- Enterprise Act of 2002

5.27 The Consumer Protection (Distance Selling) Regulations 2000 transpose into UK law the provisions of the Distance Selling Directive (97/7/EC). In line with the Directive, these Regulations impose certain obligations on the seller, such as provision of full product information, details of cost and payment, delivery arrangements and the supplier's contact details. The Regulations protect the consumer against credit or debit card fraud, and generally entitle the consumer to a cooling-off period of at least seven working days after agreeing to the purchase during which the consumer can cancel the agreement without any explanation and receive full refund. Like the Directive, the Regulations do not apply to financial services like insurance or banking which are regulated separately by the Financial Services Authority.

5.28 Similarly, the 2002 Electronic Commerce (EC Directive) Regulations, the major piece of direct regulation dealing with e-commerce, transpose into UK law the majority of

the provisions of 2000 Electronic Commerce Directive. The aim of the Regulations is to ensure the free movement of "information society services" across the European Community and to encourage greater use of e-commerce in the UK by clarifying the rights and obligations of businesses and consumers and thereby boosting consumer confidence and trust.

5.29 The Regulations establish that service providers are subject to the laws of the UK if they are established in the UK. However, online services provided from other Member States may not be subject to UK laws. Under the Regulations, the e-merchant is obliged to provider the customer with clearly defined information about the nature of its business, the commercial communication with the customer and how to complete online transactions.

5.30 The implementation of the Unfair Commercial Practices Directive, which introduces a general duty not to trade unfairly into UK law, into UK legislation by the end of 2007, and the EU's current review of the consumer law will also affect the future landscape of consumer protection legislation[33].

5.31 There are a number of statutory authorities which are responsible for upholding the provisions of domestic and European consumer protection legislation. The most notable authorities are the Office of Fair Trading (OFT) and Trading Standard Departments, both of which have powers to investigate infringements of consumer regulations[34].

5.32 More specifically, the OFT activities include:

- Promoting good trading practices through the Consumer Codes Approval Scheme
- Co-ordinating enforcement action throughout the UK with other regulatory partners
- Taking action against businesses who trade unfairly
- Providing information to help businesses to understand their legal obligations, and consumers to understand their rights and to make good choices
- Liaising with regulatory bodies in other countries that also have consumer protection enforcement powers
- Providing input to legislative changes in the field of consumer protection.

5.33 Part 8 of the Enterprise Act gives the OFT and other designated enforcers the power to seek court orders (Enforcement Orders) against businesses who breach certain consumer protection laws.

5.34 In addition to the direct regulatory measures provided by a number of laws, there is also a strong emphasis in the UK on initiatives to increase consumer awareness of how to undertake safe commercial transactions online.

[33] See http://www.dti.gov.uk/consumers/consumer-policy/eu-consumer-policy/EC-Policy-Review/index.html for more information.
[34] In Northern Ireland, the Department of Enterprise, Trade and Investment is the relevant authority responsible for enforcing consumer protection legislation.

5.35 For example, the websites www.tradingstandards.gov (run by Trading Standards Departments) and www.consumerdirect.gov.uk (run by the OFT) are dedicated to providing information to consumers and businesses on their rights and responsibilities. There is also a strong network of local trading standards offices and citizen advice bureaux to provide advice to consumers.

5.36 The OFT has developed the Consumer Codes Approval Scheme (CCAS) for approving and promoting business-to-consumer codes of practice. It aims to promote and safeguard consumers' interests by helping them identify better businesses. Code sponsors must prove their code meets the OFT's core criteria, and that their members are delivering real benefits to consumers before it is approved.

5.37 The OFT has approved five codes of practice under the CCAS. These are the Society for Motor Manufacturers and Traders; the Vehicle Builders and Repairers Association Ltd; the Direct Selling Association; the Association of British Travel Agents; and the Ombudsman for Estate Agents Company Limited. Six other code sponsors are working towards OFT approval of their codes.

5.38 The DTI has also encouraged self regulation and recommended the establishment of a self regulatory body dedicated to developing and implementing a code of best practice and seal programme for online commerce. This had led to the creation of TrustUK, a non-profit organisation led by the industry. Trust UK has developed a best practice code of conduct for e-commerce which its members agree to adhere to in return for being able to display the association's best practice seal on their website. The TrustUK seal allows consumers to identify safe traders.

5.39 There are currently four separate organisations grouped under the TrustUK brand; the Association of British Travel Agents (ABTA), the Direct Marketing Association (DMA); the Safebuy seal and the Webtrader seal. The combined membership of TrustUK is currently over 9,000 businesses.

International regulatory approaches

5.40 Across the majority of countries the same hybrid model of direct and self regulation has been used to implement consumer protection measures in the e-commerce environment.

5.41 As in the UK, the direct regulation is typically enforced via a statutory authority, which is empowered to investigate infringements of trade regulations and enforce sanctions against the perpetrators. Examples include the US through the Federal Trade Commission (FTC), Australia through the Australian Competition and Consumers Commission (ACCC) and New Zealand through the Commerce Commission.

5.42 These statutory authorities only have powers to correct violations once they have occurred and for this reason such bodies generally actively promote self regulation by the industry, aiming to encourage the use of best practice in online selling and reducing instances of trading standards infringements.

5.43 Self regulation by the industry is generally through trade associations, which promote the sharing of best practice and/or develop codes of conduct which members must adhere to. These codes of conduct typically include provisions mandating members to comply with national legislation and best practice.

Case study – the USA

5.44 In the US, for example, the Consumer Act provides legislative protection to consumers and empowers the Federal Trade Commission to enforce the trading standards. Consumers are able to complain directly to the FTC about potential infringements of trading standards and the FTC investigates, and punishes where appropriate, instances of violations. In addition, the FTC also encourages industries to self regulate by developing and enforcing their own codes of best practice.

5.45 One example is the Better Business Bureau (BBB), an independent, non-profit, membership-funded organisation which instigates consumer and business education initiatives, provides a dispute resolution service and publishes reports and business practices. The BBB's code of practice aims to ensure that members comply with trading standards regulations, and consumers can identify compliance through the Reliability seal. Currently, over 27,000 US businesses are able to display the BBB Reliability seal, which means that they must have a satisfactory complaint handling system, comply with BBB Code of Advertising and the BBB Code of Online Business Practices, and have been in existence for at least one year.

Case study – Australia

5.46 The Australian regulatory model, on the other hand, is distinct from that found in many other countries in that it places a much stronger emphasis on self regulation.

5.47 In 1999 the Australian Government issued its Policy Framework for Consumer Protection in the Context of Electronic Commerce, which established the government strategy for protecting consumers online and promoting consumer confidence. This Policy Framework established a self-regulatory approach, with the Government committing to support the industry in developing a self-regulatory system and monitor its effectiveness. It established the Expert Group on Electronic Commerce - a group of leading industry and consumer protection professionals to advise the government on e-commerce strategy – and a one-stop-shop website (consumersonline.gov.au) designed to promote e-commerce media literacy initiatives, and provide consumers with information about the e-commerce regulatory framework.

5.48 In 2000, the Expert Group on Electronic Commerce published the Australian Commerce Best Practice Guidelines, which provides an overview of how Australian e-businesses should conduct themselves online, and a framework for industry Codes of Practice. These initiatives complement the legislative framework, which includes trading standards regulations under the Trade Practices Act of 1974 and the Electronic Transactions Act of 1999, breaches of which can be enforced by the Australian Competition and Consumer Commission (ACCC).

Self-regulation and user empowerment

5.49 In order to foster confidence in the online retail environment, many countries have encouraged development of quality seals which enable consumers to recognise which vendors have committed to following a code of conduct in relation to commercial transactions on the internet. These seals are typically graphical logos which can be displayed on web trading sites of vendors who participate in industry-wide quality assurance systems. For example, quality seal systems are in place in France (L@belsite), Germany (Trustedshops) and Japan (Japan DMA), while the Global Trustmark Alliance promotes the use of quality seals at an international level.

5.50 Most countries support their regulatory systems by media literacy initiatives, which aim to educate consumers on their rights in the online commercial environment, the measures they can take to protect themselves, and the means of seeking redress in case they encounter problems. In many countries, it is the statutory authority responsible for enforcing trading standards legislation which takes responsibility for developing and implementing information initiatives and media literacy programmes, either through their website, campaigns or by publishing guidance leaflets.

5.51 In addition to the direct and self regulatory measures implemented by governments and industry, there has been a move towards user empowerment systems. These systems effectively use word-of-mouth over the internet to inform users which vendors are conforming to good businesses practices and which are not.

5.52 User empowerment systems are often used on auction sites as auction transaction often fall outside the protection of traditional regulation because the e-vendor is not entering into the transaction in the course of a business. In response, consumers have developed an alternative method of introducing consumer protection into commercial transactions with e-vendors which relies on users themselves sharing experience from their commercial transactions on the internet. The most well known example of such as scheme is that used by eBay to comment on sellers and buyers.

Case study - the eBay user empowerment system

5.53 eBay is an online auction site with a national presence in 27 countries across the globe. It has been subject to sustained growth, with net revenues growing from $1.2bn in 2002 to $4.5bn in 2005.

5.54 One of the reasons often cited by analysts when discussing the reason for eBay's success is the level of confidence consumers have in the service. This confidence is due to eBay's secure payment system, using PayPal, and its service of user rating for transactions with different vendors (positive, negative or neutral).

5.55 On completion of a transaction on eBay, both buying and selling parties are asked to provide feedback on the other. This feedback system contains two elements:

- Ratings: these can be either positive, negative or neutral
- Comments: individually posted by users.

5.56 Vendors who are consistently rated as negative by users are likely to lose customers over time while those consistently rated as positive are likely to instil more confidence especially to those new to eBay or the vendor.

5.57 The eBay user rating system is an example of an innovation to address potential consumer fears about inadequate protection. Although the system has its drawbacks and is not immune to manipulation, it is an example of successful consumer action in tackling rogue traders on the internet.

5.58 The eBay system is restricted to buyers and sellers who use the eBay auction service. However, the principle has been extended to the general online shopping environment. User rating of online shopping services has emerged through websites offering comparison services for different retailers. An example of this system in practice is Resellerratings.com.

Case study – the Resellerrating.com user empowerment system

5.59 Resellerratings.com is an example of an online store comparison service, which provides users with comparative information about different online shopping services, including key purchasing information (for example, whether credit cards are accepted, length of delivery etc.) as well as user ratings of different vendors.

5.60 Like eBay, the user rating system comprises of two elements; an individual user's comments and a rating across five areas:

- Pricing of products and services
- Likelihood of future purchases
- Shipping and packaging
- Customer service
- Return and replacement.

5.61 Such user-implemented regulatory systems are for many online shoppers the key method of differentiating between multiple retail services.

Fraud using the internet

5.62 The internet has become a major conduit for fraudulent activities, or scams. Such scams vary in nature, although they usually involve the consumer handing over their financial details or money to partake in 'too-good-to-be-true' offers or 'get-rich-quick' schemes.

5.63 Such activities are almost universally illegal, either through legislation aimed specifically at internet fraud or through the extension of offline laws online, with perpetrators subject to civil or criminal prosecution. The enforcement of the legislation is usually through the criminal law system, though often also involving statutory bodies responsible for the direct regulation of trading standards. There is also a strong emphasis on raising consumer awareness, aiming to educate consumers to identify scams before they become victims of them.

5.64 However, and as has been discussed earlier in the section on identity theft, there are limits of what can be done at a national level. The nature of the internet is such that internet scams are often based in a different country from that where the intended target resides. This makes international cooperation crucial to effective law enforcement. As in the case with the enforcement of trading regulations internationally, discussed in the previous section, this includes cooperation and knowledge-sharing between national agencies.

International framework

5.65 As in the case of trading regulations infringements, it has generally been recognised that combating internet fraud effectively requires international cooperation, especially as many internet scams will have repercussions outside of the country of origin of perpetrators. To this end, inter-governmental initiatives have been established to facilitate information sharing and cooperation in investigations across national borders.

5.66 A major inter-governmental initiative tackling the issue of internet fraud is ICPEN, which was discussed in the previous section. ICPEN's remit extends to sharing information and cooperating in preventing internet fraud. Its consumer portal, e.consumer.gov, collects complaints about consumer fraud both within and across countries. ICPEN has also initiated internet fraud specific activities, the most recent being the 2006 International Sweep Day held as part of the Scams Awareness Month in February 2006[35].

5.67 The initiative involved volunteers from member countries sweeping the internet to identify 'too-good-to-be-true' internet scams such as work-at-home schemes, lottery scams, pyramid schemes, get-rich-quick schemes, prize or free offers on the web and educational offers. As a result of the initiative, 440 letters were issued to traders in ICPEN jurisdictions and 320 sites were either closed or amended, including 5 court actions.

UK regulatory approach

5.68 In the UK, offline fraud legislation extends to the internet, as discussed in the previous section. Although the criminalisation of SPAM has had a significant impact on reducing the ability of internet fraud scams to be propagated, internet fraud remains a growing concern. Recent research has found that 83% of the UK population feel they do not know enough about how to protect themselves online, with 42% of the population relying purely on friends and family for online safety advice rather than seeking out expert information[36].

5.69 The key statutory authority which investigates scams involving deceptive and misleading trading practices in the UK is the Office of Fair Trading. The OFT can use its civil enforcement powers under the Enterprise Act to tackle many scams. Other authorities are also able to investigate where the fraud falls specifically within their remit, including:

- The Financial Services Authority (FSA) for scams involving fraudulent investment activities
- The Advertising Standards Authority (ASA) for scams involving misleading advertising.

5.70 In addition, the National Hi-Tech Crime Unit, part of the UK National Crime Squad, has a specific remit to investigate fraud allegations.

5.71 Apart from direct regulation, there are numerous information initiatives which aim to educate consumers about internet fraud and how they can protect themselves. For example, the OFT held Scams Awareness Month in February 2005 and 2006, which included radio advertising, web chats, press releases and poster/leaflets being distributed.

5.72 The Government has also recently launched an initiative to raise public awareness of the issues of email viruses, e-crime and online fraud, and provide advice to consumers on solutions. As discussed earlier, the Get Safe Online website, www.getsafeonline.org, provides advice to consumers on how to spot scams and how to safeguard themselves. The campaign is a joint initiative between HM

[35] See http://www.oft.gov.uk/News/Press+releases/2006/35-06.htm for more information.
[36] Get Safe Online

Government, the National Hi-Tech Crime Unit, and private sector sponsors from the worlds of technology, retail and finance, including BT, Dell, eBay, HSBC, Lloyds TSB, Microsoft, MessageLabs, securetrading.com and Yell.com.

International regulatory approaches

5.73 Like the UK, the majority of countries have criminalised internet fraud, and its primary delivery mechanism SPAM, either through specific legislation or through the extension of offline legislation into the online environment.

5.74 In most countries, enforcement of legislation relating to internet fraud is carried out by the same statutory authority responsible for enforcing trading standards. In specific cases, it is possible for other relevant statutory bodies to become involved if the scam has a particular relevance to them. For example, scams relating to misleading advertising often involve the enforcement body responsible for advertising standards, while those relating to financial services involve the financial sector authority.

5.75 Many countries have also criminalised SPAM, one of the main conduits for internet fraud, via primary legislation, and have encouraged the industry to develop mechanisms for blocking SPAM.

5.76 Information initiatives and media literacy schemes have also emerged alongside regulation to educate consumers on how to avoid become victims of internet fraud. Techniques for doing this often include special web pages devoted to information about scams, and tips on how to avoid them.

Case study - Australia

5.77 Australia serves as an example of a common model, which is replicated elsewhere in the world, in countries including the US, New Zealand and Canada. The Australian regulatory system for controlling internet scams involves two core elements:

- Investigation of potential scams by the relevant enforcement authorities
- Media literacy initiatives to educate consumers in how to identify potential scams.

5.78 Consumers are able to report internet scams to the Australian Competition and Consumers Commission (ACCC), which will investigate and potentially prosecute perpetrators. The Australian Securities and Investment Commission (ASIC) also receives and investigates incidents of scams, although only when they are strictly related to financial investments.

5.79 The ACCC maintains a Consumers Online website which provides up-to-date information on the latest scams and aims to educate consumers on how to identify them while ASIC maintains a consumer education area on its website, including ‘pie in the sky’ competitions which award prizes to consumers who provide information on the most outrageous scams encountered on the internet.

Conclusion

5.80 The UK approach involves a substantial amount of consumer protection legislation some of which specifically applies to distance selling including that over the internet. Much of the UK legislation is European in origin and is, therefore, harmonised with legislation in other Member States of the EU.

5.81 The growth in B2C e-commerce may offer some evidence that consumers are developing greater trust in the online environment. The extensive online presence of many traditional bricks and mortar companies with established trust relationships, as well as the establishment of successful online brands, has increased consumer confidence in making online commercial transactions.

5.82 Nevertheless, there remains the potential for less scrupulous businesses to exploit end users, especially in cases where anonymity and reputation are more difficult to judge – these risks are to some extent inherent in the impersonal and global nature of the internet. The ongoing promotion of self-regulatory approaches, such as TrustUK, will play a part in building customers confidence that they are dealing with a bona fide merchant. The opportunity the internet affords the consumers to exchange information and experience means that user empowerment schemes, such as rating systems, will also continue to be provide an additional layer of the consumer protection framework.

Section 6

Content and contact

6.1 The internet as a global network of networks brings together a global user base with a global set of content and services. Specifically, internet access allows any member of society from almost anywhere in the world to gain access to content and services produced by anyone and hosted anywhere on the global network.

6.2 This freedom to consume and offer content and services from anywhere across the global network brings with it a number of consumer benefits. It increases choice and offers opportunities to interact with other users in innovative new ways, whether by sharing own content or participating in online communities. It does, however, also raise some important consumer protection concerns.

6.3 The most serious and high profile issues include the distribution of child abuse images, the exposure of children to harmful (sexual and violent) content and the use of internet chatrooms by paedophiles for grooming children. There are also many other issues associated with minors' use of the internet, including their access to illegal services such as gambling.

6.4 There has been widespread reporting on these issues highlighting the prevalence and seriousness of the issues:

- Child pornography: BT reported in December 2005 that its "cleanfeed" technology blocks an average of 45,000 attempted hits onto illegal child pornography sites each day[37]
- Internet gambling: In a recent survey, only 7 out of the 37 gambling sites tested refused to allow access to a user providing only a Solo card as age verification. Solo cards can be issued to children as young as 11[38]
- Internet advertising: 20% of adverts on a child-orientated games site were promoting gambling services, which would be illegal for their underage viewers to use.[39]

6.5 Whilst the issues are numerous and diverse in nature, there are four key groups of issues we have focused on:

- Child contact - Online grooming (through chat rooms, instant messenger, forums, community websites)
- Illegal and harmful content for children - Pornography, violent images, bad language, instructional websites as well as use of age-restricted services
- Inappropriate content and services for the general public – Distribution of child pornography, internet advertising standards etc.

[37] BT. See http://www.btplc.com/societyandenvironment/news/showarticle.cfm?articleid=2ab29f02-bd0c-4e0a-952f-60fef2500246
[38] Kids Online
[39] NCH, GamCare, Citizen Card Report 2004

- Online gambling.

Child contact

6.6 Child contact issues and in particular, the exposure of children to unwanted solicitation or grooming by sexual predators via online communication activity through, for example, chat rooms, forums, instant messaging, community websites and online games, is a key concern worldwide, with many domestic markets conscious of the need to ensure that children are not exposed to harmful situations, either online or offline, as a result of their internet activity.

International framework

6.7 Most of the work done at international level in relation to child contact issues has focused on encouraging the development of self-regulatory measures and media literacy campaigns instead of introducing primary legislation.

6.8 Self-regulation and the use of technology have emerged as primary ways to manage children's exposure to both online content and contact as it requires participation of a wide range of players at different parts of the value chain. The most common self-regulatory measures include:

- Chat room and content filtering: this refers to restricting access to certain websites, using techniques to screen sites' text for instances of forbidden words or content. Such filtering can be done by the ISP directly, as would be the case with BT Cleanfeed, or by the internet users themselves using content filtering software

- Moderation: this involves including an adult moderator in an online chat room or forum environment to monitor the activities taking place and step in where there is potential that a child is at risk

- Classification: this involves classifying websites into genre or age categories to indicate the type of content or activities taking place (e.g. a forum chat site may be classified as a 15, indicating that the subject matter or nature of chat is inappropriate to persons under the age of 15).

6.9 Media literacy schemes are playing an increasingly important role in any strategy to ensure a safe online environment and protect children. They empower consumers and allow them to take appropriate action to prevent exposure to harmful content and contact.

6.10 The EU's approach to the issue is stated in its Safer Internet Plus Action Plan which is a part of a set of measures taken by the EU to deal with illegal and harmful content on the internet. The aim of the Safer Internet Plus Action Plan is to promote safer use of the internet and new online technologies, including mobile and broadband content, online games, peer-to-peer file transfer, and all forms of real-time communications such as chat rooms and instant messages. Its primary focus is on improving the protection of children and minors, and it aims to achieve that through four main actions:

- Fighting illegal content – this will involve providing funding for hotlines that would enable the public to report illegal content and which would pass the reports on to the appropriate body for action

- Tackling unwanted and harmful content – this will involve funding for technology that enables users to limit the amount of unwanted and harmful content they receive, or that can be used to test the effectiveness of available filters

- Promoting a safer environment – this will involve providing a Safer Internet Forum for national co-regulatory or self-regulatory bodies to exchange information and experience

- Awareness-raising – this will involve support for information exchange on how to make interactive and mobile applications safe for consumer.

6.11 The latest programme of actions was initiated in 2005 and is due to run for four years. It follows a similar plan of action that ran between 1999 and 2004.

6.12 The European Commission has also launched INSAFE, a network of national organisations that coordinate internet safety awareness in Europe and act as an information resource. INSAFE partners work closely with each other to share best practice, information and resources as well as interact with industry and consumers. INSAFE promotes the development of information literacy and provides consumers with means of reporting harmful or illegal content and services. Its awareness raising campaigns have covered issues as wide as cyber-bullying, online privacy and chatting and are aimed at audiences of different ages, both minors and adults.

6.13 There are many other examples of self-regulatory initiatives that exist at an international level. Below is a small sample of those initiatives.

Childnet (Industry watchdog)

- Created the Chatdanger website – targeting children to educate them about how to keep safe in online arenas

- Developed Netbenefit Programme to inform parents & children about online dangers

- Lobbied for warning mechanism in children's chat rooms.

Virtual Global Taskforce

6.14 This is an international alliance of law enforcement agencies including the National Crime Squad, US Department for Homeland Security and Interpol.

- The taskforce has taken a central role in both overt and covert monitoring of chat rooms as a means of identifying potential groomers

- One of the VGT's key initiatives, led by the Australian High Tech Crime Centre and due to go live in April 2006, is for 24/7 overt online presence, equivalent to offline 'bobbies on the beat' schemes whereby police from each member agency visit chat rooms and other online areas where children could be potentially at risk.

Wired Safety

6.15 This is a global consumer support group that is run entirely by volunteers who patrol the internet in search of child molesters and cyberstalkers (Wiredcops.org). It also

provides educational material for children about online dangers and how to counteract them.

UK regulatory approach

6.16 Home Office records indicate that there were over 16,000 reported incidents of crimes against children in the reporting year 2004/05[40]. Although the figures do not reveal the number of incidents that were initiated over the internet, it is generally recognised that the internet poses a growing risk for minors.

6.17 The anonymity of the internet has allowed paedophiles to contact children without having to identify themselves first, and build up a relationship with them for the sole purpose of persuading them into sexual activity. The techniques which sex offenders use to entice children into sexual activity are known as "grooming". Online grooming is a grave concern – unlike in an offline world, where opportunities for adult strangers to be alone with children do not occur easily, in the online world they are an everyday possibility.

6.18 Online contact with minors raises the possibility of illegal activity both online, in case of solicitation of children by sexual predators in chat-rooms and other anonymous forms of communication, and offline, in case of a meeting occurring between the child and paedophile who has established contact via an online communication arena. As a result, direct regulation is in place in the form of primary legislation.

6.19 Until 2003, the Indecency with Children Act of 1960 was the key piece of legislation used to prosecute incidences of child molestation via the internet. Under this act, 'any person who commits an act of gross indecency with or towards a child…or who incites a child…to such an act….shall be liable on conviction to imprisonment for a term not exceeding two years'.

6.20 Although this Act could have in principle extended to cover the offence of online grooming, it had a number of significant shortcomings which made successful prosecution under the Act difficult. For example, the perpetrator could not be charged under the Act if the prosecution could only show the evidence that that the perpetrator had a general intent to persuade the minor into committing a sexual act. Rather, a charge under the Act required prosecution to prove that the perpetrator had intention to commit a specific act of indecency, that is, the prosecution was required to show that there was "an act of gross indecency" which the child was being incited to allow or participate in.

6.21 In order to address the shortcomings of the Indecency with Children's Act, in 2003 the Sexual Offences Act was passed which introduced online grooming as a new criminal offence, punishable with between 7-10 years imprisonment. In addition, any adult logging onto an internet chat-room under the pretence of being a child or teenager could be subject to a civil preventative order under the Sexual Offences Act.

6.22 Enforcement of this legislation is the role of the police and the criminal law system. Some tactics employed by the police to catch online groomers include covert sting operations, with police officers posing as children in online chat rooms, as well as overt police presence online. For example, the National Crime Squad has developed

[40] The Home Office statistics

a ‘bobbies on the beat’ scheme which uses explicit police presence in online chat rooms as a deterrent to potential child groomers.

6.23 There are, however, inevitable limitations on the effectiveness of these mechanisms, due to resource constraints, the potential risk of entrapment via sting operations, and difficulties proving intent without risking harm to the child. For that reason, the involvement and cooperation of the industry is key to empowering users and ensuring a safe online environment for some of the internet’s most vulnerable users.

6.24 The most significant initiative in the UK is the Home Office Internet Task Force for Child Protection. The Task Force was established in 2001 in response to a report by the Internet Crime Forum which highlighted the importance of taking additional security measures in order to protect children on the internet. The Task Force brings together the government, law enforcement agencies, industry representatives and child welfare organisations.

6.25 The key objective of the Task Force is to allow the stakeholders to share information and knowledge on the keys issues relating to child protection online, and develop approaches for tackling them. The Task Force is active in a number of different areas:

- It provides good practice guidance for the industry including advice on chat rooms, instant messaging and web-based services that encourage clear safety messages, and user-friendly ways of reporting abuse

- It provides guidance for parents and children on how to stay safe on the internet. For example, it runs a website for young people with information and advice on how to protect themselves - thinkuknow.co.uk

- It has set up the Child Exploitation and Online Protection (CEOP) Centre, operational from April 2006 (www.ceop.gov.uk). The Centre will provide a single point of contact for the public, law enforcers and the communications industry to report targeting of children online and will offer advice and information to parents and potential victims of abuse 24 hours a day. The Centre will also work with police forces around the world.

6.26 As an additional element in the strategy to protect minors from inappropriate online contact, the government has developed a series of information campaigns, aimed at educating end-users so that they know both how to avoid exposure to harmful contact in the first place and the complaint procedure should such exposure take place. These schemes have included:

- A major advertising campaign (television, radio and online) warning of the dangers of internet paedophiles launched by the government in 2003 and aimed at educating parents and children about safe usage of the internet

- The Scottish Executive’s ‘Think You Know’ advertising scheme of 2004 which warned children and their parents about the potential danger of grooming in internet chat rooms.

6.27 Various children’s charities also work on internet safety issues in the UK. The Children’s Charities’ Coalition for Internet Safety, for example, is a grouping of major

children's charities that campaign on internet issues. Expert resources that are available to download include a CHIS Digital Manifesto for Child Safety Online[41], and NCH's Child Abuse, Child Pornography and the Internet report[42].

International regulatory approaches

6.28 Primary legislation relating to the protection of children from contact with adult sexual predators in the offline world is well established in most national markets. In some markets the existing legislation already covers child contact facilitated by the internet. In others, like in the UK, amendments or new legislation has been passed to extend the applicability of the law into the online world. Australia and the United States are two such examples.

6.29 In Australia, legislation exists to protect minors from illegal online contact and extends to offline meetings with paedophiles arranged via an internet chat room. Since most criminal activities are handled by state law, such legislation varies by state. However, most territories have introduced specific laws to counteract the use of the internet to entice a child into a sexual act.

6.30 In the United States, legislation exists to deal with illegal activity as a result of online contact with children. Federal law enforces a maximum sentence of 15 years for anyone who 'knowingly persuades, induces, entices or coerces' any child to engage in any sexual activity. Most state laws are even more specific in relation to such activity in the online domain. For example, Georgia state law states it is unlawful for "any person intentionally or wilfully to utilize a computer online service…to seduce, solicit, lure or entice' children".

6.31 Whilst most national markets have passed legislation against child contact, there are significant limitations both in the use of primary legislation, and in the scope of the legislation. As in the UK, the courts have encountered difficulties establishing intent to commit a criminal offence, and law enforcement services have faced ethical dilemmas when considering whether to allow a meeting between a potential paedophile and child to take place. Most national laws have limited success in preventing online grooming from taking place.

6.32 Consequently, in most markets the legislative approach is supplemented by a series of self-regulatory and media literacy initiatives which draw more extensively on industry and end-user participation. Such initiatives tend not to deal specifically with just online contact but encompass a range of issues dealing with illegal and inappropriate content and contact over the internet. These initiatives are discussed in full in the next section.

Case study - Taiwan

6.33 An example of such a self regulatory initiative is Taiwan's Website Ratings Promotion Foundation. It was established in November 2004 to take responsibility for providing a safe online environment for children. It includes representatives from the Ministries of Education, Transportation and Communications, industry players such as Chunghwa Telecom, Yahoo!, Kimo and Microsoft and various social welfare groups.

[41] See http://www.nch.org.uk/uploads/documents/Digital_Manifesto_web.pdf for more information.
[42] See http://www.nch.org.uk/uploads/documents/children_internet_report_summ.pdf for more information.

6.34 As a result of the initiative, youth protection zones now feature on the front pages of many websites in Taiwan, targeted at both children - reminding them of the potential dangers they could face online - and parents - providing them with information about how to protect their children online. ISPs in Taiwan have also agreed to launch youth protection hotlines which concerned parties will be able to call to register complaints.

6.35 In addition, information campaigns, such as the Information Month held in December 2004, have played a central role in Taiwan's minor protection strategy. During the Information Month, exhibitions on internet safety were held in a number of cities featuring government agencies, ISPs and web content providers. The focus of the exhibitions was on providing information and advice to parents on how they can best protect their children from dangers encountered on the internet.

Conclusion

6.36 Child contact has been an area of key concern in the UK in recent years. Consequently, the UK has taken key steps to address the issue, including a legislative approach, a policing/enforcement regime, industry initiatives and government led media-literacy programmes.

6.37 Ongoing media-literacy is key to the continued success in this area reinforcing the sense of being safe and vigilant on the internet in the minds of young children. This will require ongoing initiatives and monitoring as new generations of users begin to use the internet.

Illegal and harmful content for children

6.38 The distinction between illegal and harmful content is important as the two types of content are dealt with differently:

- Illegal content must be dealt with at source by the police and the legal authorities whose activities are covered by national legislation and legal cooperation agreements. However, the industry can be of considerable assistance in restricting the circulation of illegal content

- Harmful content is both content which is authorised but has restricted circulation (e.g. for adults only) and content which could be offensive to some users, even if publication is not restricted because of freedom of speech.

6.39 The terms illegal and harmful have the potential to extend across three areas:

- Exposure of children to harmful or illegal material - this relates largely to website content which would be deemed harmful for minors or impressionable minds (e.g. adult or extremely violent content) or which is illegal (e.g. child pornography)

- Access to illegal services/goods – this relates to access to age restricted services/ goods (e.g. age rated content, alcohol, cigarettes and online gambling). The key concern in this area is online gambling since alcohol and cigarettes are physical items requiring time to deliver and for which the determined child has relatively easier offline alternatives and more immediate means of purchase

- Exposure of children to harmful advertising - the harmful nature of advertising can arise from the ad itself being harmful or the product/good being advertised

being harmful for the target audience. The regulatory approach is distinct from that of other material and, therefore, is discussed separately (albeit briefly) in this section.

6.40 The focus of this section is on the first of these three issues, namely, the exposure of children to harmful and illegal material.

International framework

6.41 The EU's approach to protecting minors has focused on encouraging member states to adopt self-regulatory solutions and initiate media literacy schemes to empower end-users, rather than create primary legislation. Hence, the EU has passed a variety of secondary legislation relating to the protection of children online, with a focus on self-regulatory and media literacy solutions.

6.42 In September 1998, the EU passed the Recommendation 98/560/EC on the Protection of Minors and Human Dignity in Audiovisual and Information Services which offered guidelines for the development of national self-regulation in the protection of minors, for example, the development of codes of conduct by ISPs.

6.43 The EU's preference for self-regulation and end-user empowerment was consolidated in the 2002 European Parliament's (EP) Resolution on the Protection of Children Using the Internet, which reaffirmed the full responsibility of parents for protecting children using the internet. The EP's resolution precluded the use of obligatory content blockers as a means of protecting children from unsuitable online material and called on ISPs to adopt self-regulation to ensure the safety of minors on the internet.

6.44 This was supplemented in 2004 with the additional Recommendation on the Protection of Minors and Human Dignity in Audiovisual and Information Services which focused on enhancing media literacy and encouraging cooperation between self-regulatory and co-regulatory bodies in member states, and the exchange of best practices such as the rating and classification of content.

6.45 Additionally, the EU launched the Safer Internet Action Plan in 1999, and its successor, the Safer Internet Plus Action Plan, in 2005 to promote safer use of the internet by combating illegal and harmful content on global networks. The plan promotes industry content-monitoring schemes, especially dealing with content such as child pornography and racism, and encourages development of filtering tools and rating mechanisms. It plays an important role fostering international cooperation on the issue of illegal and inappropriate content.

6.46 Beyond the EU, there are other international bodies which have sought to create self-regulatory mechanisms for limiting access to harmful content for children. One such body is the Internet Content Rating Association (ICRA). ICRA does not itself engage in rating internet content. Instead, ICRA encourages content providers to self-classify their content using ICRA's rating system. This rating system in turn enables the end-users to use filtering software to block access to any websites which they deem undesirable based on the rating information.

6.47 However, the take-up and application of the system has been limited. Although over 100,000 websites worldwide have already self-labelled using ICRA's rating system, including brand names such as Microsoft, AOL, T-Online and Hustler, representing

millions of web pages, they represent only a tiny proportion of the entire world's 85m domain names[43]. The ICRA system has to date only been translated into three languages - French, German, and Spanish – which further limits its application internationally.

6.48 In addition to government initiated regulatory measures, the internet industry has developed tools to enable the filtering of content deemed inappropriate for minors. Primarily, industry initiatives have been developed at three layers in the internet value chain - the search engine layer, the access layer and the client application layer:

- Search engines: Many search engines, including Google and Yahoo!, have developed 'safe search' options which allow users to set their search preferences to exclude explicit adult content
- Access/ISP layer: Many ISPs offer web filtering as a value added service, with individual subscribers able to choose their own settings. An example of this is AOL's Parental Controls, which has three settings (kids only, young teens, mature teens) which vary the level of filtering of sites (including chat services)
- Client applications: Individual users are able to install software on their computer which will filter web content, often allowing them to create different user identities with different security settings.

UK regulatory approach

6.49 The UK's approach to protecting minors from illegal and harmful content and contact broadly mirrors that advocated by the EU in its Action Plan on promoting the safe use of the internet. Thus, in the regulation of harmful and illegal content, the focus has been on self-regulation and the use of technology together with information campaigns and media literacy strategies that empower end-users to assume responsibility for their own protection.

6.50 Self-regulatory schemes which have developed in the UK are exemplified by a range of ISPs and ICHs, including Yahoo! UK's appointment in 2001 of an adviser whose remit included improving safety of children using its chat services[44], and Wanadoo's age control devices Additionally, there are joint industry-government initiatives such as The Home Office Internet Task Force for Child Protection on the Internet (discussed in previous section in relation to child contact).

6.51 UK ISPs have also created the Internet Service Providers Association (ISPA), a trade association responsible for co-ordinating the industry, particularly in relation to the protection of minors. ISPA has an established Code of Practice which members must comply with in return for being entitled to use the ISPA logo. ISPA has over 120 members, including all major and middle tier UK ISPs. Their Code of Practice has two core principles relating to the protection of minors from illegal and harmful content:

- Encouraging the emergence of enabling technologies which give the consumer or parent a choice as to what content they receive (e.g. filtering technologies)

[43] The Verisign Domain Name Report November 2005
[44] These arrangements have now lapsed

- Placing responsibility on the provider of content to ensure that the content is legal, but also suitable for the intended audience.

6.52 Members who violate the code can be suspended by the ISPA Council.

6.53 End users, however, play a key role in monitoring and regulating the content available to minors on the internet. There is a plethora of filtering tools, including NetNanny and Cybersitters, available to parents and guardians, and most ISPs offer optional functionality to limit the scope of content that can be accessed from the internet.

6.54 The challenge to date has been in ensuring that parents and guardians are aware of tools available to them, and have the knowledge and the means to implement them. A recent study indicated that 46% of parents in the UK used some filtering services, with many parents also reporting that they find the use of such applications challenging[45]. For that reason, schemes such as the getsafeonline.com programme will provide a useful and increasingly important resource for parents to help them understand what they can do to protect their children and how. It will also be crucial to ensure that all parents have adequate levels of media literacy.

International regulatory approaches

6.55 Few markets have adopted a purely legislative approach towards regulating children's access to illegal and harmful content. Australia and the US are examples of countries that have passed primary legislation, but have subsequently shifted to a greater reliance on co-regulatory and self regulatory regimes.

Case study - Australia

6.56 In Australia, an initial attempt by the government to regulate material harmful for children was in the form of primary legislation, in the 1999 Broadcasting Services Amendment (Online Services) Act.

6.57 The legislation originally proposed included a requirement on ISPs to block adults' access to specified content on sites outside Australia and imposed a penalty of AUD$27,500 per day for non-compliance. The proposals were met by strong criticism. Many organisations such as the EFA (Electronic Frontiers Australia) held that the restrictiveness of the proposed Act amounted to an internet censorship law that was not present in any country democratically and politically comparable to Australia. The industry objected that blocking access to content at the ISP server level is not technically and commercially feasible as the Act stipulated.

6.58 As a result, the legislation was amended during its passage through Parliament to remove the requirements for censorship of content via blocking of sites. The Act still defines certain types of internet content as prohibited content (or potential prohibited content) but instead offers the industry two choices:

- To develop a Code of Practice compliant with the Act for approval by the Australian Communications and Media Authority (ACMA), or

- To comply with an ACMA "Industry Standard" which would be developed in the absence of a Code or if a registered Code of Practice was found to be deficient.

[45] UK Children Go Online, April 2005

6.59 The ACMA is the statutory body responsible for the enforcement of the Act. End-users can register complaints about specific internet content with the ACMA which the ACMA will investigate. Where appropriate, the ACMA can issue notices to ISPs/ICHs to take action to remove such content. Non-compliance with an ACMA notice is an offence which attracts a significant financial penalty.

6.60 Under the revised act and codes of conduct, ISPs and ICHs are required to take reasonable steps to:

- Provide a regulator-approved restricted access system for content classified R18 that is, suitable for those over 18 years of age (requiring sites to collect personal information from visitors e.g. copy of driving license, birth certificate or credit card details) before allowing them access to R18 content
- Ensure internet access accounts are not provided to children under 18 without parental consent
- Encourage commercial content providers to use appropriate labelling systems in hosting content which is likely to be considered unsuitable for children (e.g. the PICS rating system)
- Provide users with information about supervising children's access to internet content, and the ACMA complaints procedure
- Make available to subscribers an IIA family friendly filter service
- Comply with take-down notices issued by ACMA.

6.61 This approach has led to industry-led innovations such as the internet Industry Association (IIA) Family Friendly ISP seal programme, launched in March 2002, which provides a visible symbol (the Ladybird Seal) to show which ISPs are compliant with the IIA codes.

Case study – the USA

6.62 The US has attempted to pass several pieces of legislation targeted specifically at child protection on the internet. However, most of these attempts have faced barriers as they are deemed to be in conflict with the constitutional right of US citizens to freedom of speech.

6.63 The 1996 Communications Decency Act (CDA), prohibits the distribution to those under 18 years of 'any material that… is offensive as measured by contemporary community standards, sexual or excretory activities or organs'. This Act was partially overturned by the Supreme Court which blocked the portion of the CDA relating to 'indecent speech', ruling it an unconstitutional contravention of the First Amendment right to free speech.

6.64 The 1998 Child Online Protection Act (COPA) was intended to protect children from harmful sexual online material but was similarly blocked by a Supreme Court ruling that the law was likely to be unconstitutional.

6.65 The 2002 Dot Kids Implementation and Efficiency Act creates a kids.us domain that would only have material appropriate for children under 13 and would not allow any access to chat rooms. However, this bill created huge controversy from those who

objected to the idea that the government should set the standards for what constitutes appropriate content.

6.66 In the meantime, a number of self-regulatory initiatives have had successful implementation:

- The development of PICS (Platform for Internet Content Selection), a new internet protocol for labelling online content, developed in collaboration with industry players and end-users
- The establishment of conventions for content label formats and standards for the distribution of label information.

6.67 The movement towards self-regulation has been reinforced by the enhanced consumer awareness that has been generated by consumer empowerment initiatives such as for example GetNetWise, an online resource for parents with information on consumer content filtering products, law enforcement contents and recommendations of age-appropriate content.

Case study - Italy

6.68 The Italian model of minor protection from illegal and harmful online content and contact represents a hybrid of government involvement and self-regulation, rather than a standalone self-regulatory model as found in some other parts of Europe.

6.69 The Italian government (via the Ministry of Innovations and Technology and Ministry of Communications) has promoted the concept of self regulation through the Internet e Minori Code. This code requires industry players to create and implement self-imposed rules, and aims to allow minors to use the internet in a safe way and defend their rights to privacy. It also aims to ensure more effective cooperation in preventing and punishing cybercrime that involves children (e.g. child pornography).

6.70 Compliance with the code is monitored by the Comitato di Garanzia Internet e Minori (Committee for the Implementation of the Internet and Minors Code) which receives and manages complaints about potential violations and warns the perpetrators where necessary. It also provide support to ISPs and ICHs in adopting the Code and monitors the application of the code.

6.71 In addition to direct regulation, the Italian model has also focused on end-user empowerment through initiaitives such as the:

- CORECOM's (Regional Committee for Communication) initiative, Internet e minori: navigazione sicura (The internet and minors: safe surfing)
- Il Filtro system, produced and distributed by commercial business websites which acts as a filter to block messages and content that may be harmful to children.

Minors' access to online gambling services

6.72 The protection of children from online gambling services is a specific issue in the markets where gambling via the internet has been legalised. In other markets, where online gambling services are illegal, minors' access to gambling services is part of a wider issue of preventing access to such services for all users, regardless of ages. We consider these markets later in this section.

6.73 Online gambling is legal in the UK and there is, therefore, a clear need to ensure that minors are restricted from accessing such sites. In the UK, 2005 Gambling Act is the basis of a direct regulatory framework. The Gambling Act:

- Prohibits anyone under 18 from gambling online
- Requires UK-based gambling sites to ensure sufficient age-verification mechanisms are in place to prevent under-age participation, for example credit card checks.

6.74 Nevertheless, despite the presence of age-verification systems designed to block accounts for under-aged users at the point of registration, research by public welfare groups such as the NCH, the children's charity, has shown that children as young as 11 have successfully set up gambling accounts on UK websites. A 2004 report jointly compiled by NCH, GamCare and CitizenCard found that only seven of 37 gambling websites tested stopped a 16 year-old applicant from registering her details online using her Solo card as age-verification[46].

6.75 Such findings highlight the fact that any successful counteraction of online gambling by minors relies on a variety of players rather than any one individual. Thus the government, industry players, banks and credit card companies, as well as end-users and their parents, all have a role to play in protecting children.

6.76 End-user blocking techniques in particular offer parents and guardians the opportunity to impose access controls for services intended only for those over 18 years of age. There are currently a number of such blocking services available on the market, including standalone blocking software such as CyberSitter or NetNanny, online blocking services provided ISPs as well as content portal or integrated browser-blocking software.

Inappropriate content and services for the general public

6.77 The definition of what constitutes inappropriate content varies by country and even region. Whilst in one country certain types of content are deemed perfectly legal and acceptable for consumption, in others, production or consumption of the same content may be frowned upon or even be a criminal offence. These variations in attitudes occur for many reasons, including local political, cultural and religious differences, and result in different stances on how best to tackle the distribution of what is considered inappropriate content within each individual territory.

6.78 There are, however, certain types of content for which there exists a widespread consensus amongst different countries of what is deemed to be "decent" or "legal". The best example of such content where there is a general consensus is child pornography. In such cases, a cross-border approach to tackling the distribution of such content is possible. For other types of content, national differences in attitudes make it difficult to achieve cross-border cooperation, forcing national markets to adopt solutions tailored to their specific circumstances and prevailing cultural norms.

6.79 The extent and nature of international and national legislation and regulation differ across content types, with certain types of content being targeted more actively than others. For the purposes of this report, we have considered online dissemination of inappropriate content separately from online advertising that contravenes formal

[46] NCH, GamCare, Citizen Card Report 2004

regulation or ethical standards. Broadly speaking, inappropriate content can cover the following types of content:

- Child pornography
- Content and communications which facilitate acts of terrorism
- Racist or xenophobic material, or material which incites racism or xenophobia
- Other content (includes adult pornography, violent material, defamatory content and other content which may be deemed to be illegal or inappropriate under a nation's laws).

International framework

Inappropriate content

6.80 Child pornography is the clearest example of content that is considered not only inappropriate but also illegal in most countries. At an international level, both the Council of Europe and the United Nations have taken action against dissemination of child pornography, and have encourage collaboration between nations in combating the problem.

6.81 The 2000 UN Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, mandates signing parties to prohibit the sale of children, child prostitution and child pornography within their nation's law, including via the internet. It also provides a framework for increased international cooperation in prosecuting perpetrators in these areas. The Protocol has entered into force following 12 ratifications by signing nations.

6.82 The 2001 European Convention of Cybercrime mandates signing parties to prohibit the production, distribution and buying of child pornography over the internet. It was the first international treaty to criminalise offending behaviour directed against computer systems, networks or data in addition to content related crimes such as child pornography. The Convention creates a legislative framework for investigating and prosecuting violations of law with respect to child pornography, and mandates cooperation between national agencies in combating child pornography. It entered into force in July 2004 following 5 ratifications. To date, it has been signed by 38 countries and ratified by 12 countries, though not including the UK.

6.83 The substantive criminal law measures of the Eurpean Convention of Cybercrime include offences on:

- Intentional illegal access of computer systems
- Intentional illegal interception of non-public transmissions of computer data
- Intentional interference with computer data including deletion or alteration
- Intentional interference with a computer system.

6.84 Additionally, the Convention includes crimes such as computer related forgery and fraud, and content related offences such as child pornography. Offences related to infringements of copyright and related rights are also included within the Convention.

6.85 Attempts to encourage international collaboration for other types of inappropriate content have proved problematic due to national differences in the definition of what is inappropriate. For example, the committee drafting the Cybercrime Convention discussed the possibility of including content related offences other than child pornography (Article 9) within the Convention, for example, the online distribution of racist propaganda. However, the committee could not reach consensus on the inclusion of additional offences within the Convention. Instead, it was recommended that additional protocol to the Convention be developed under the title "Broadening the scope of the convention to include new forms of offence".

6.86 The Additional Protocol concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems aims to harmonise substantive criminal law in the fight against racism and xenophobia on the internet and, to improve international co-operation in this area. Following five ratifications, it came into force on 1 March 2006. Importantly, however, the UK and the US are currently not signatories to the Additional Protocol.

6.87 Though the US had signed the original convention which focused on child pornography, it has not signed the Additional Protocol on the grounds that the Protocol restricts an individual's right to free speech. The First Amendment of the US Constitution guarantees an individual's right to free speech and is broader in scope than the equivalent Article 10 of the European Convention of Human Rights. The First Amendment states that 'Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances'.

6.88 Such differences in national opinion compromise the effectiveness of the treaty. Websites containing offensive content, in this instance racist or xenophobic content, can relocate their hosting to a country which is not a signatory to the treaty thereby avoiding legal sanctions.

Online advertising

6.89 For inappropriate advertising practices on the internet, there is a European coordination manifested through the EU's Television without Frontiers Directive and the European Advertising Standards Alliance (EASA).

6.90 The EU's Television without Frontiers Directive was first written into EU law in 1989. Since then it has been subject to a number of amendments with a substantive review of the legislation currently underway. The Directive seeks to harmonise Member States' legislation across all aspects of the production and distribution of audiovisual media, including advertising.

6.91 When the legislation was first established, it was primarily aimed at linear audiovisual content, that is, transmission of broadcast television via a terrestrial, satellite or cable network. The current review of the Directive seeks to address the increasing role of the internet as a platform for the delivery of audiovisual services. The new Directive has not yet been finalised.

6.92 Under the proposed new Directive, the regulations would not apply to:

- Internet services whose primary objective is not the provision of audiovisual services (e.g. contains an audiovisual content clip which is ancillary to the main purpose of the site)

- Electronic versions of newspapers or magazines
- Private correspondence (e.g. e-mail).

6.93 The provisions of the proposed TVWF Directive in relation to advertising include:

- Ensuring that commercial communications are clearly identifiable
- Ensuring that commercial communications do not:
  - Use subliminal techniques
  - Include racial, sexual or national discrimination
  - Offend religious or political beliefs
  - Encourage behaviour prejudicial to health or to safety
  - Encourage behaviour prejudicial to the protection of the environment
  - Include commercial communications related to tobacco products

6.94 The European Advertising Standards Alliance does not have a Code of Conduct which members agree to comply to. Instead, it works as a forum and lobby group for self-regulatory entities from across Europe and other member countries, and industry players such as advertising federations. Since 1992 it has also had a role in handling and resolving cross-border complaints concerning advertising content and standards between members. Its remit extends into the internet space.

UK regulatory framework

Inappropriate content

6.95 In the UK, content deemed illegal under the Obscene Publications Act and the Public Order Act of 1986, the relevant offline legislation, is also illegal in the online context. There is no specific legislation relating to inappropriate content for adults in the online world.

6.96 In addition to the above legislation, the UK has encouraged the development of self-regulatory mechanisms for dealing with inappropriate content encountered on the internet. The main organisation engaged in this area is the Internet Watch Foundation (IWF) which has been established with the purpose of eliminating images of child pornography hosted anywhere in the world, as well as criminally obscene and criminally racist content hosted in the UK.

6.97 The IWF works in partnership with the government, law enforcement and the wider industry, and acts as a hotline for reporting illegal and obscene content on the internet. It also provides useful information for internet users on how to protect themselves online using filtering services and other available tools.

6.98 The IWF acts by issuing take-down notices to hosting service providers relating to content which has been reported to it, has been ascertained by IWF to be illegal, and is hosted in the UK. If the content is illegal but hosted outside the UK, the IWF notifies the relevant authorities in the country of jurisdiction.

6.99 The IWF also maintains a database of all IP addresses hosting illegal content both in the UK and internationally. The IWF regularly updates the database and distributes it to all UK ISPs who can voluntarily choose to block their users' access to the listed addresses. The Internet Services Providers Association (ISPA), the key UK industry association, indicates that all major ISPs as well as most smaller ones, covering the vast majority of consumer internet connections, have implemented the database or will shortly be doing so. In addition, the IWF supplies ISPs with details of online user groups dedicated to disseminating illegal and offensive material, and recommends that they be blocked by ISPs.

6.100 The IWF also assists law enforcement agencies dealing with illegal content. It passes details of reports relating to potential child abuse either to the UK law enforcement agencies, for content hosted in the UK, or to the relevant national hotline or agency, for content hosted outside the UK.

6.101 The IWF has been immensely successful in its strategy to restrict access to illegal content on the internet hosted in the UK. In 2005, only 0.4% of potentially illegal child abuse images reported to IWF were hosted in the UK[47].

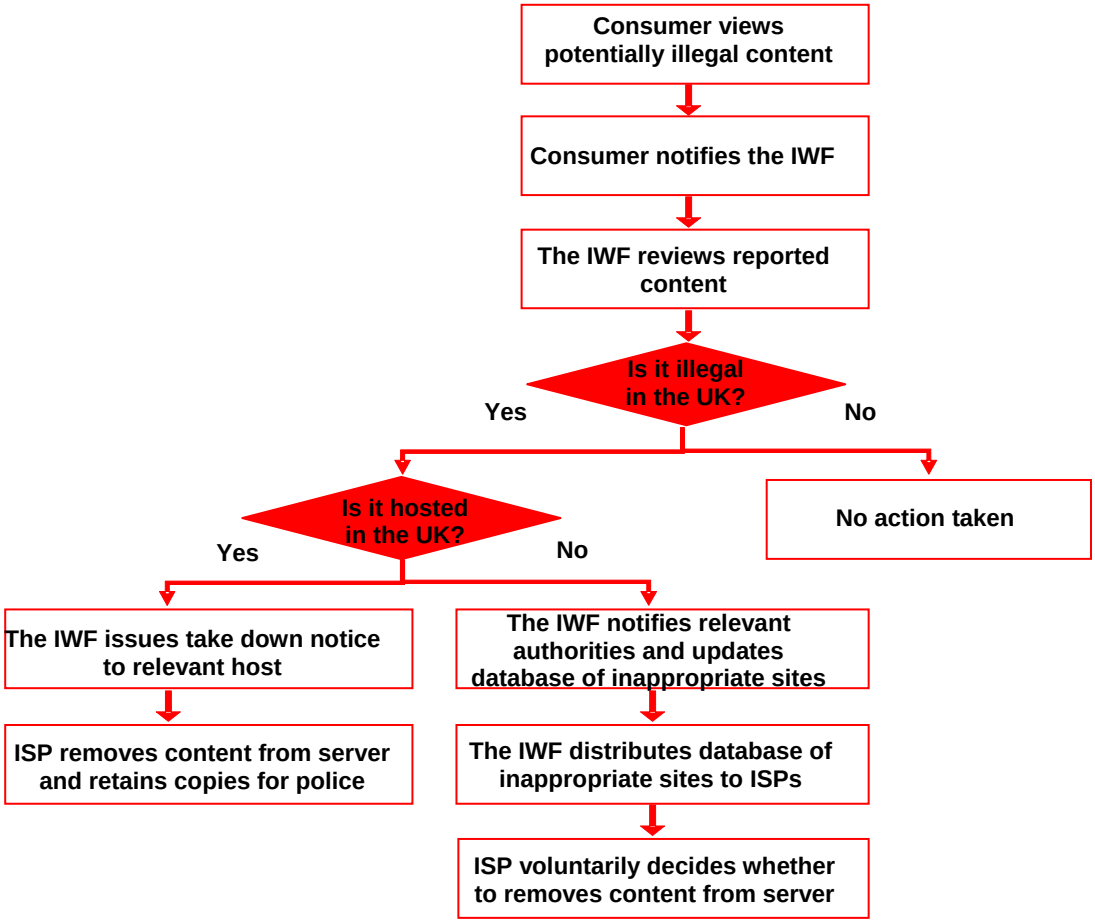
6.102 The work of the IWF is supported by other self-regulatory initiatives. The ISPA has developed its own Code of Practice to deal with the issue of inappropriate content which all its members adhere to. This Code of Practice mandates members to comply with take-down notices issued by the IWF and requires ISPs to provide relevant user details to the police.

6.103 ISPA also urges its members to provide sufficient information about filtering tools to all their customers. Non-compliance with the Codes of Practice is subject to sanctions, which may include suspension of membership.

6.104 The coordination between the IWF and the ISPs is illustrated in the exhibit below.

[47] Internet Watch Foundation

Figure 6.1: The IFW process for handling reports of illegal content



Online advertising

6.105 In relation to inappropriate advertising practices, the UK has a self regulatory system for dealing with internet advertising, which falls under the remit of the Advertising Standards Authority (ASA), an independent body established by the advertising industry. This body is responsible for administering a code of practice, developed by the Committee of Advertising Practice (CAP), which is an industry body whose membership includes many major advertising and marketing industry organisations.

6.106 The Code of Practice covers a broad spectrum of media advertising, including both online and offline methods. It specifically includes online advertising such as banner and pop-up adverts. In case of complaints, the ASA instigates an investigation and rules whether to uphold the complaint or not. Where appropriate, the ASA can implement sanctions. In case of persistent offenders, the ASA can refer the case to the OFT.

International regulatory approaches

6.107 Other European markets have also opted for self-regulatory mechanisms to deal with inappropriate content, as illustrated by the examples of France and Sweden discussed below.

Case study – France

6.108 The French system of internet regulation in relation to inappropriate content has similarities with the UK in that the internet industry body, AFS (Association des Fournisseurs d'Access et de Services Internet) has developed its own code of conduct to deal with content considered illegal under French law. However, whereas in the UK the industry code of conduct mandates members to comply with an independent, non-governmental agency, the IWF, in France the code mandates members to comply with legal authorities when dealing with illegal content. The French ISPs are required to provide filtering software to all their users.

6.109 Like the IWF does in the UK, the AFA maintains a point of contact for the public to report instances of potentially illegal content. Following notification, the AFA passes on details of the content to the French authorities. If the content is hosted in France, the French authorities will ask the relevant ISP to take down the content. If the content is hosted outside of France, the French authorities may notify the relevant authorities in the country of the host about the content.

Yahoo!com versus the French Government

6.110 In France, the legal framework around incitement of racial hatred is particularly strong. This has led to challenges in cases where content hosted abroad has been deemed illegal in France. The most famous example of this involved the French government attempting to force Californian-based Yahoo!.com to block the access of French internet users to auctions of Nazi memorabilia (illegal under French law). The French government threatened to issues Yahoo!.com with a non-compliance penalty of up to €100,000 a day.

6.111 In response, Yahoo!.com filed a law suit to the Californian state court, complaining that the French government had no jurisdiction over a US based company. The complaint was upheld by the court, which also ruled the French ruling as unconstitutional.

6.112 Since then, French legal authorities have moved away from issuing fines, and have instead sought to work with the relevant authorities from the host nation to see if there are any diplomatic means by which the content, illegal under French law, can be removed from the overseas host.

Case study – Sweden

6.113 The Swedish regulatory system has involved the use of government legislation to force the industry into developing self-regulatory mechanisms to deal with illegal content on the internet.

6.114 The Responsibility of Electronic Bulletin Boards Act, passed by the Swedish Parliament in 1998, places the responsibility for control and monitoring of illegal content on the content hosts. In effect, it makes content hosts legally responsible for the content they host. However, in a later clarification it was decided that content hosts would not be held liable "ex ante" unless they failed to act following a customer complaint, thus removing the emphasis of legal responsibility from the content hosts to the content owners.

6.115 As a result, the industry has established its own system of regulation which uses the non-profit industry group, BitoS, as the forum for developing codes of ethics for

content providers, portal operators and internet service providers alike. BitoS' members are obliged to abide by notice and take-down requests issued to them.

Case study - Australia

6.116 The approach to content considered illegal under Australian law differs from that adopted by the UK and many other European countries. The Australian Communications and Media Authority (ACMA), the relevant regulatory body, takes a more direct role in combating dissemination of illegal content.

6.117 In 1999, an amendment to the Broadcasting Services Bill implemented a strict regulatory system which empowered the Australian Communications and Media Authority (ACMA) to regulate online content hosted within Australia. Under this regulation, content which would fall under specific classifications in the Office of Film and Literature Classification (OFLC) scheme used for films, DVDs and video games is prohibited online.

6.118 Unlike in the UK, it is the regulator rather than an industry association / charity which deals with internet user complaints. Upon receiving complaints that such content exists, ACMA is empowered to issue and enforce take-down notices to Australian ISPs. For content hosted outside Australia and which ACMA deems to be illegal, ACMA notifies the relevant authorities in the host countries and also instructs Australian ISPs to block access to the content.

6.119 In addition to this direct regulatory approach, the Internet Industry Association (IIA) has developed its own Code of Conduct which applies to all internet content hosts and service providers in Australia. This requires members to comply with ACMA procedures and provide filters to all subscribers.

Case study - China

6.120 Some other markets such as China have taken a strong interventionist approach to blocking content deemed illegal or inappropriate. Furthermore, Chinese legislation allows for any player in the value chain involved in delivering such contact to be prosecuted.

6.121 Within the Chinese internet regulation system, there are seven different government entities with some jurisdiction, including the General Administration of Press and Publication, the Ministry of Public Security and the State Secrecy Bureau. The legislation covers many different levels of the internet value chain, including Internet Service Providers (ISPs), content providers and end users.

6.122 Under existing laws, ISPs are legally responsible for the content they host. Failure to comply with government regulations can result in a loss of operating license and arrests of company staff. Providers of online bulletin boards or forums must prominently display government usage guidelines on their sites, control access and use of their services using secure login details, and maintain usage records for 60 days.

6.123 Filtering takes place primarily at the backbone level of China's network, while individual Internet Service Providers also implement their own blocking. Search engines filter content by keyword and remove certain search results from their lists. Similarly, major Chinese blog service providers either prevent posts with certain keywords or edit the posts to remove them.

6.124 A recent addition to the Chinese internet is Google.cn, which has agreed to censor its search results to comply with government regulations. However, the company will not be launching other services, such as email and blogging, over concerns that it will be forced to disclose personal information of its users.

Case study – regulation via localised search engines

6.125 Another self-regulatory method of restricting access to illegal content has involved localised search, that is, search engines filtering search results to exclude sites which may be deemed inappropriate in a specific local area. An example of this is filtering search by Google in France and Germany, that is, Google.fr and Google.de respectively.

6.126 In addition to its main search engine, google.com, Google operates a number of national sites, including google.co.uk (for the UK), google.ca (for Canada), google.fr (for France) and google.de (for Germany). The use of local search sites enables Google to filter out certain sites to comply with national laws. A significant proportion of sites to which access is denied in this way contain pro-nazi, white supremacist material, which is banned in both Germany and France.

Online gambling

6.127 Generally, in all countries where internet gambling is legalised, it is also directly regulated. In some markets, however, such as the United States and Australia, internet gambling remains illegal, even though it continues to take place, having proved difficult to eliminate.

International framework

6.128 Due to significant differences in the treatment of internet gambling services across markets, there is currently no cross-border legislation relating to online gambling.

6.129 The one exception is the Council of Europe's Convention on Information and Legal Cooperation Concerning Information Society Services. This Convention mandates signatories to exchange drafts of any domestic legislation with regards to the provision of online services, and to cooperate where possible in developing such legislation.

6.130 The treaty will enter into force once there have been 5 ratifications, at least one of which is by a State which is not a member State of the European Economic Area. To date, there have been two signatories and one ratification only.

UK regulatory approach

6.131 The UK is one of the most liberalised markets for online gambling. The regulatory approach is based on direct regulation. Under current legislation, the 1968 Gaming Act and the 1976 Lotteries and Amusements Act, UK citizens are able to use all gambling and gaming internet services except for gaming services hosted in the UK.

6.132 This anomaly is being addressed in the reforms under the Gambling Act of 2005, which will allow for UK gaming services to be hosted in the UK. In addition, the Gambling Act will set up a sector regulator, the Gambling Commission, and require UK hosted operators of gambling of services to acquire a licence from the Gambling Commission. The Gambling Commission will ensure that all licensed services meet

certain technical and legal standards, and will investigate all complaints from the users. The Gambling Act will come into force in 2007.

International regulatory approaches

Case study – France

6.133 The French online gambling and gaming market is strictly regulated by the Ministère de l'Intérieur, the French equivalent to the UK Home Office, and was for a long time a monopoly market. The Act passed in 1930 gave Pair Mutuel Urbain (PMU) a monopoly position to provide betting services for horse racing. In 2001, la Francaise des Jeux, a semi-public company (72% stake held by the State), was launched to provide online gambling and gaming services for French residents. These two providers are currently the only two entities which are legally allowed to provide online gambling and gaming services in France.

6.134 However, the advent of the internet has made this duopoly policy harder to police, as overseas companies are able to provide gambling and gaming services to French residents without having a physical presence in the country. This has led to a recent dispute between PMU and a Maltese gambling company, as detailed below.

6.135 PMU recently sued a Maltese Company, Zeturf Ltd, for breaching trade laws in France. Zetuef Ltd is registered in Malta and licensed by the Lotteries and Gaming Authority (LGA) of Malta. Its servers are based in Malta and formally all its customer transactions take place there.

6.136 However, the French courts ruled that Zetuef Ltd was contravening French law by operating in France, and issued it with a penalty notice of €50,000 a day to stop working. In addition, French courts issued a court order to Bellmed, the company providing co-location facilities to Zeteuf Ltd, ordering them to stop serving the Zeteuf Ltd or risk fines. Zetuef Ltd now plans to use Maltese Courts to appeal the decision and the case will provide an important test of current French approach to regulation of online gambling.

Case study – Sweden

6.137 The regulatory framework for internet gambling and gaming in Sweden is very similar to that in France in that only certain types of companies are licensed to offer services. The Lotteries Act of 1994 and the Casinos Act of 1999 stipulates that only certain types of companies are allowed to offer gambling and gaming services: those established by the horse racing industry, the Swedish State, and organisations that will benefit the public. In principle, commercial bodies are excluded from being able to provide such services. The responsibility for regulating online gambling comes under the Loteriinspektiorien (National Gaming Board).

6.138 The effect of this legislation has been to create an oligopoly market in the provision of gambling services. The market is dominated by two players: Svenska Spel (a state owned company) and Trav och Galopp, a company owned by the horse racing industry. Recently, the Swedish Government refused to provide a licence to Ladbrokes, a UK based company. This ruling is being challenged on the grounds that it runs against EU competition law.

6.139 A recent review of the Swedish online gambling sector, commissioned by the Swedish Government and published in January 2006, stated that there was unlikely to be a realistic way of stopping offshore online betting companies from targeting

Swedish consumers. This may signal a change in the current legislative position in the near future.

Case study – the USA

6.140 The legislative and regulatory environment for internet gambling in the US is exceedingly complex, and both the federal and state governments have jurisdiction. Importantly, online gambling is currently illegal in the USA.

6.141 At a federal level, the Wireline Act of 1961 bans interstate sports betting. Since online sports betting is assumed to be interstate, it is thus deemed illegal. However, the federal position on other forms of interstate gambling and gaming is unclear, with several different bills having an application in the online gambling and gaming environment.

6.142 The original intention of all these acts was to enable individual States to govern the gambling sector as they saw fit. Thus, the current approach varies from state to state. In Nevada, State Authorities have handed over the regulation of the internet gambling market to an independent body, the Gambling Commission, which maintains a list of approved gambling and gaming websites. In contrast, Washington State has passed legislation explicitly banning internet gambling and making the user of such services liable for prosecution.

6.143 Given this plethora of different federal and state laws, the US position on online gambling is increasingly unclear. It is likely that a review of existing regulation will be instigated in the near future, with a view to achieving a consolidated and aligned policy across the country.

6.144 Adding to the calls for greater clarity is the 2005 ruling by the World Trade Organisation (WTO). This ruling was a response to an action brought against the United States by Antigua, which complained that the U.S. federal and state anti-internet gambling regulations violated the United States' obligations under the WTO, and that such policies had decimated its burgeoning internet gaming industry. The WTO ruled in favour of Antigua and was upheld by the Appellate Panel, the final panel of appeal. The US had until 6th April 2006 to respond to this decision, and the true ramifications of the ruling have yet to be ascertained.

Section 7

Malicious computer activity

7.1 This section sets out the consumer protection issues surrounding malicious computer activity in the form of internet-sourced attacks on computers. In this section we focus on two important types of malicious computer activity which can cause consumers considerable harm:

- Physical attacks on computer in the form of hacking and malware
- Rogue internet diallers

7.2 In this section, we do not discuss computer-based attacks committed for commercial gain, such as phishing and scam via email, which are covered in Section 4.

Physical attacks on computers

7.3 Physical attacks on computers manifest themselves in two ways, although, as discussed later in this section, the approaches to tackling them are broadly similar:

- Hacking – gaining unauthorised access to computer systems with the intention of stealing/corrupting data, disabling a website or hijacking equipment in the networked home. These attacks tend to have specific targets
- Malware – the infection of random targets via viruses, worms or Trojan horses

7.4 Traditionally, the main targets of hacking activity have been corporate organisations and government institutions. However, hacking is increasingly emerging as an important consumer protection issue especially with new types of attacks such as the hijacking of equipment in the networked home. As the focus of this study is on consumer issues, this section does not deal with the issue of hacking on corporate computers and websites. Furthermore, the discussion on malware in this section excludes adware which is discussed in Section 4 of the report.

7.5 The threat posed by both hacking and malware is considerable and has been widely studied and reported:

- In the US, approximately 59m US adults have some form of malware on their computers. In addition, in 2003/4, US consumers are estimated to have spent more than $2.6 billion in protection software and $9bn in for computer repairs, parts, and replacement to solve problems caused by viruses and spyware[48]
- In the 2003 CSI/FBI Computer Crime and Security Survey, viruses were the most cited form of attack with 82% of respondents being affected at an estimated cost of $27m[49].

7.6 The risks to end users arising from hacking and malware are increasing as hackers become more sophisticated in their techniques. Today's malware attackers rely less

[48] Pew Internet & American Life Project
[49] CSI/FBI Computer Crime and Security Survey 2003

on viruses and more on worms which, unlike viruses, do not require human action (e.g. opening an e-mail attachment) to become operational, and tend to spread automatically through any uprotected connections on the network.

7.7 Additionally, the mass take up of always-on broadband has led to increased attacks on unprotected home networks.

International framework

7.8 There have been a number of international efforts to standardise national legislation dealing with malicious computer activity. The Council of Europe's Convention on Cybercrime, signed in November 2001 by 30 countries including the US, Canada, Japan and South Africa in addition to the European members of the organisation, was the world's first international treaty to address the issues of malicious activity on computer networks. It came into force in 2004.

7.9 The main objective of the Convention is to pursue a common criminal policy against cybercrime based on fostering international cooperation and harmonising domestic law provisions. Accordingly it places certain key obligations on all national signatories, including the requirements to:

- Establish laws against cybercrime
- Ensure that their law enforcement authorities are equipped with the necessary procedural capability to investigate and prosecute cybercrime offences
- Provide international cooperation to other countries in their efforts against internet-based crime.

7.10 Amongst the activities that the Convention criminalises are:

- Intentional unauthorised access of a computer system (Article 2)
- The intentional damaging, deletion, deterioration, alteration or suppression of computer data (Article 4).

7.11 These activities correspond broadly to the offences of hacking and malware distribution respectively.

7.12 Additionally, the European Electronic Crimes Task Force (EECTF) was established to facilitate cross-national cooperation further by putting cybercrime investigators directly in touch with their international counterparts.

7.13 The task force is an online community delivered via a secure portal in which individuals from European law enforcement agencies, military forces and academic institutions are able to come together in a secure environment to share knowledge and expertise about malicious computer activity. Although industry players are eligible to join, they are only able to do so if they are sponsored by an existing member.

7.14 Another example of trans-national cooperation involves the 14 member countries of the Southern Africa Development Community (SADC), including Zambia, Mauritius, Swaziland and South Africa. In May 2005, these countries agreed to standardise their cybercrime laws to enable more effective prosecution of cross-border computer-based crimes by, for example, allowing easier extradition within the SADC region.

7.15 Despite this agreement, in practice it has been difficult to achieve harmonisation in the case of the SADC countries. Some members of the Community, such as Botswana, currently have no legislation in this field. Even where national laws do exist they often differ widely in key areas, for example with respect to their length of sentencing of hackers and malware distributors.

7.16 These initiatives have significantly helped the cross-border prosecution of hackers and virus creators, but do not address all the limitations of the legislative approach, notably the need to stem the dissemination of viruses in the first instance.

7.17 Since the threat posed by hackers and malware exploits technological vulnerabilities in the individual software, industry players are increasingly looking to self-regulatory mechanisms to address these risks. Indeed, industry players have been the most vocal in their opposition to state-based legislative regulation of the internet.

7.18 In the 2000 G8 Cybercrime Conference, for example, the Global Internet Project, a group of industry executives, challenged the vision of a state-led approach to addressing the problem of malicious computer activity, and called upon the G8 to adopt self-regulatory mechanisms rather than legislation which, they argued, stifled free access to the internet.

7.19 Additionally, many in the industry hold that industry players themselves are better equipped to develop means of preventing security breaches before they happen, rather than wait for law enforcement agencies to act in the aftermath of criminal attacks already committed.

7.20 There are three types of industry players who potentially have a role to play in this area. These include:

- Security and anti-virus firms (e.g. Qualys, Symantec and Sophos)
- Software vendors (e.g. Microsoft)
- ISPs.

7.21 Security and anti-virus firms and software vendors have assumed some responsibility in the fight against hacking and malware distribution, while ISPs have often been the channel through which such products have been distributed to end customers. There is a large number of anti-virus software products available on the market, and while rival vendors typically compete fiercely against each other in their marketing, the highly competitive dynamic is supplemented by a more cooperative information-sharing process whereby industry players inform each other as soon as a new virus has been identified.

7.22 A recent example of such cooperation is the secureIT Alliance, comprising companies such as Microsoft, Symantec, McAfee and Panda. It was formed as a way for industry players to pool their resources to provide security solutions for the Microsoft platform in particular, by sharing information about developing threats and best practices, particularly in relation to newer issues such as spyware.

7.23 The legislative and industry-focused strategies have also been supplemented by media literacy initiatives which focus on end-user empowerment and education as a means of tackling the threats posed by malware and hacking. Indeed, research has shown both the need for, and potential success of, media literacy schemes as a

means of educating consumers about the threats posed by viruses and malware in general.

7.24 For example, the Pew Internet and American Life Project study conducted in July 2005 demonstrated the extent to which internet users have become more attuned to the threat posed by viruses and malware as more information on the risks they pose has become available to them:

- 81% claimed to have become more cautious about e-mail attachments, fearing the possibility of a virus
- 48% stopped visiting websites they fear may contain viruses or other unwanted programmes
- 25% stopped using file-sharing software which often comes bundled with adware
- 18% have switched internet browser software as a result of virus attacks[50].

7.25 There are numerous media literacy initiatives at national and international level. A notable example is the European Network and Information Security Agency (ENISA)

7.26 ENISA is a high-tech crime agency established by the EU in November 2003 to help educate the public about viruses, denial of service attacks and other online threats. It collects and analyses data on security incidents and emerging risks, and tracks the development of standards for products and services on the internet. ENISA is also the coordinating agency for Europe-wide investigations into virus outbreaks.

UK regulatory approach

7.27 UK consumers are highly concerned about malicious computer activities. Though many consumers have been subject to a virus attacks, there is a low awareness of how to deal with the problem.

7.28 According to a Home Office survey, almost a fifth of households (18%) where the respondent had used the internet at home reported that their computer had been affected by a computer virus in the past year. 87% of those surveyed rated securing their computer from viruses as one of their top security priorities[51]. A different survey found that 17% of UK adults rated internet crime (hacking, viruses and malware) as their number one concern, greater than their concern about potential physical crimes offline[52].

7.29 Consumer awareness in this area is still limited; a report produced by Get Safe Online found that 52% of those surveyed felt they had 'little or no knowledge' of safe computing practices. Indeed, only 32% of respondents updated their anti-virus software at least every three months, rendering their computers vulnerable to attack[53].

[50] Pew Internet and American Life Project
[51] The Home Office Fraud and Technology Crimes Report 2003
[52] Get Safe Online
[53] Get Safe Online

7.30 In the UK, a range of primary legislation exists to deal with criminal activities such as hacking and virus dissemination. The Computer Misuse Act (CMA) (1990) is the central piece of legislation pertaining to the misuse of computer systems. In Section 1 it criminalises 'unauthorised access to computer material' which covers hacking and in Section 3, it prohibits 'unauthorised modification of computer material' which covers the distribution of viruses.

7.31 Several virus developers have been sentenced to prison under the terms of Section 3, the first case being the 18 month imprisonment of Christopher Pile, the 'Black Baron', in November 1995. More recently, Simon Vallor was sentenced under Section 3 to a two-year custodial sentence in January 2003 for writing and disseminating three computer viruses (Gokar, Redesi and Admirer).

7.32 The CMA is policed by the Computer Crime Unit of London's Metropolitan Police. The majority of cases referred to it involve hacking, virus development and distributed denial-of-service attacks. Additionally, several local forces across the UK are also developing their own cybercrime units.

7.33 As the CMA was passed in 1990, it did not specifically address the internet or the concept of networked computer systems. It is currently perceived to be somewhat vague in terms of the legality of denial-of-service attacks: while certain aspects of denial-of-service attacks clearly fall under the provisions of the CMA, others are not so obviously accommodated.

7.34 As a result, in 2004 the All Party Internet Group published its review of the legislation and outlined its suggested ideas for improvement. These recommendations resulted in the drafting of the Computer Misuse Act 1990 (Amendment) Bill which sought to amend the CMA to ensure its compliance with the European Convention on Cyber Crime. It called for the maximum prison sentence for breaching section 1 of the Act to change from six months to two years and the criminalisation of denial-of-service attacks by the inclusion of a specific Denial of Service offence. In the event, the Bill failed to receive Royal Assent because Parliament was prorogued.

7.35 Under the Terrorism Act 2000, the definition of terrorism is widened to include actions that 'seriously interfere with or seriously disrupt an electronic system'. Consequently anyone who endangers lives by manipulating computer systems would face prosecution under the Terrorism Act.

7.36 Proposals outlined in the Police and Justice Bill in January 2006 seek to toughen up cybercrime laws by increasing the maximum prison sentence for hacking from five to ten years and putting in place mechanisms that facilitate cross-national extradition. Clause 35 of the bill also calls for the banning of the development, ownership and distribution of 'hacker tools' but has been criticised for failing to differentiate sufficiently between tool used for legal as well as illegal purposes (such as the distinction between a password cracker and password recovery tool for example).

7.37 The UK regulatory approach has been supplemented by industry-based and media literacy initiatives. The Internet Crime Forum (ICF) is an example of a UK based organisation that actively seeks the involvement of key industry players. Alongside law enforcement agencies, the CPS, the Home Office and the DTI, the ICF also comprises industry bodies such as ISPA, Linx and ISPs. Its stated aim is to encourage cooperation between the various players 'develop[ing] and maintain[ing] a working relationship between the Internet Service Providers Industry and Law Enforcement Agencies in the UK, such that criminal investigations are carried out

lawfully, quickly and efficiently while protecting the confidentiality of legitimate communications and with minimum impact on the business of the industry'.

7.38 The Home Office has been particularly active in launching initiatives to educate consumers about how best to protect themselves from malicious computer attacks. In April 2001, it funded the establishment of the National High-Tech Crime Unit (NHTCU) which has since engaged in a variety of media literacy programmes.

7.39 Most recently, as we discussed earlier, in 2005 the Home Office launched the Get Safe Online campaign as a joint initiative between the Government, the NHTCU and private sector sponsors including BT, Dell, eBay, HSBS, Message Labs and Microsoft. Get Safe Online aims to raise public awareness of the issues surrounding malware by providing easily accessible advice on its website (www.getsafeonline.com), specifically targeted at home users.

7.40 In February 2005, the Home Office also helped launch IT Safe, a free rapid alerting service run by the National Infrastructure Security Coordination Centre (NISCC) that informs home PC users about serious internet security problems such as viruses and software vulnerabilities both on its website and via an e-mail or text alert system that users are invited to sign up to.

International regulatory approaches

7.41 In most markets primary legislation, whether involving the amendment of existing laws to accommodate the online environment or the creation of new laws specifically designed to combat cybercrime, exists as a deterrent to, and means of prosecuting, hackers and virus developers.

Case study – the USA

7.42 The US government has been one of the most active worldwide in terms of passing laws to counteract hacking and malware attacks. The Computer Fraud and Abuse Act of 1984 represented the launch of federal US cybercrime law and is an example of an approach involving the development of legislation specific to cybercrime.

7.43 However, although this law was groundbreaking as a single piece of legislation that specifically targeted computer-related offences, its focus is very much on corporate computers as opposed to home PCs. This specific law criminalises activities designed to access a 'federal interest computer', which is defined as one used by a financial institution or the US government. In other words, the law served primarily to safeguard digitally stored government and financial information, as opposed to purely consumer information. Hence its impact on consumers remains limited.

7.44 In October 1996, the National Information Infrastructure Protection Act was enacted as part of Public Law and expanded upon the Computer Fraud and Abuse Act. Amendments touched upon the availability, confidentiality and integrity of computer networks, thereby broadening the definition of computer hacking punishable by law to encompass more consumer-centred issues such as password security. Furthermore, in order to extend the law's coverage, 'federal interest computer' was replaced with the term 'protected computer'.

7.45 In July 2002 the House of Representatives approved the Cyber Security Enhancement Act as a standalone bill. In November 2002, the Act passed the Senate as an amendment to the Homeland Security Bill. This Act:

- Gives the police additional powers to perform internet eavesdropping without first obtaining a court order
- Allows ISPs to disclose information about subscribers to law enforcement authorities
- Provides for a maximum life prison sentence for those convicted of malicious hacking.

7.46 In addition, most states have enacted internet laws which have tended to develop alongside and reflect federal legislation. Particularly significant here has been the anti-spyware legislation that has emerged at a state, as opposed to federal, level. Although federal legislation does exist in the form of the internet Spyware (i-SPY) Prevention Act of 2005, new state legislation has developed that complements this. An example includes the Alabama Consumer Protection Against Computer Spyware Act which prohibits wilfully using computer software to take control of another computer. Similarly, the Illinois Spyware Prevention Initiative Act prohibits anyone other than the authorised user of a computer from copying computer software onto the computer.

7.47 Despite the extent of primary legislation in the US, there have been a number of challenges. One such challenge relates to potential contradictions in the US legislative landscape whereby laws such as the Uniform Computer Information Transactions Act (UCITA) could be interpreted as making it easier for hijackers and virus developers to launch their attacks, thereby compromising the effectiveness of legislation designed to curtail such activity. The UCITA allows software developers to put backdoors into programmes so they can be remotely disabled (e.g. in the case that a customer has not paid for the software). However, this capability could open up the opportunity for hackers to exploit the backdoor mechanism to corrupt or crash the software.

Conclusion

7.48 Difficulties in prosecuting serve as a key obstacle to the successful implementation of legislation aimed at malicious computer activity. The sheer number of malicious attacks makes enforcement and prosecution an enormous task, particularly given the significant evidential challenges resulting from the fact that hackers are typically highly adept at covering their tracks and virus-developers usually employ obfuscation techniques such as self-encryption and self-decryption to conceal viruses from direct examination.

7.49 Moreover, domestic legislation cannot be effective in the absence of a complementary international legislative framework, since differences in national legislation allow cyber-criminals to simply move their operations to another country to avoid prosecution. Without trans-national cooperation between law enforcement agencies, identifying and prosecuting cyber-criminals becomes far more problematic, as was compellingly demonstrated by the recent Sasser virus case; in the absence of a single European police force with whom to negotiate, the FBI and CIA had to liaise with a local police force in Northern Germany to arrest the perpetrator which slowed down the process.

Rogue internet diallers

7.50 Diallers are forms of software that can be transmitted through the internet. Diallers switch the modem setting of the computer that the dialler programme is running on

from a particular internet connection to a different one. In the UK, the switch has historically been from a local rate ("0845") telephone internet connection to a premium rate ("090" or equivalent) connection.

7.51 Diallers can be a legitimate and convenient way of paying for content on the internet – such as sports results, sites for charity contributions, music downloads and adult services – using premium telephony charges rather than credit or debit cards.

7.52 The way that diallers typically work is that on accessing a website which contains a dialler, a consumer is shown a pop-up or dialogue box which asks whether they wish to download and install a dialler programme. The key terms and conditions such as the cost should also be present. If the user clicks the "yes" box, the dialler programme installs itself in the consumer's computer. The programme switches the user's computer to a premium rate internet connection, allowing the consumer to be charged to view/access the website content.

7.53 The dialler programme should uninstall itself after the content or service has been provided and paid for, and return the customer's modem to its previous setting. However, there exists a type of rogue dialler using premium rate (numbers beginning with "09" in the UK), international and satellite numbers that acts as a serious virus and can result in substantial levels of consumer harm. The two most significant problems with rogue internet diallers are:

- Failure of diallers to uninstall themselves when commanded to do so by the consumer (after legitimate use), resulting in continued use of the modem being charged at the higher rate; or

- Dialler programmes installing themselves surreptitiously when the consumer is connected to the internet. This typically involves the use of pop-up windows on the computer screen to trigger the surreptitious installation, even if the only action the consumer takes is to attempt to close the pop up window. The user will then run up large bills for internet access unknowingly.

UK regulatory approach

7.54 The regulatory framework for Premium Rate Services (PRS) is set out in Sections 120 to 124 of the Communication Act 2003. The regulatory arrangements for PRS follow a self- and co-regulatory approach with the primary role for consumer protection assigned to the Independent Committee for the Supervision of Standards of Telephone Information Services (ICSTIS) which is an industry-funded regulatory body.

7.55 ICSTIS regulates by enforcing a Code of Practice which includes a requirement for PRS providers to make an announcement concerning the call rate and the prescribed maximum call duration (twenty minutes) on opening the call. ICSTIS also has the power to impose a range of sanctions on services that breach the Code according to the seriousness with which it regards the breach. The sanctions range from obtaining assurances about future behaviour and instructing refunds to be offered to imposing fines, barring access to services and prohibiting certain "named" individuals from operating services for a set period.

7.56 Ofcom's involvement in the PRS regulatory regime is to provide statutory "backstop" support to the work of ICSTIS. Ofcom enforces directions issued by ICSTIS through Ofcom's condition regulating the provision, content, promotion and marketing of PRS

("the PRS Condition") under Section 120 of the Act. The PRS Condition requires all communications providers to comply with the provisions of the ICSTIS Code.

7.57 Rogue internet diallers resulted in substantial levels of consumer harm during 2004. Between August 2003 and July 2004, ICSTIS received around 60,000 individual consumer complaints, approximately two-thirds of which related to diallers. As a result, in August 2004, Ofcom undertook a review of the regulatory framework for PRS in order to assess whether consumers were adequately protected from the potential for consumer detriment involving PRS.

7.58 The Ofcom report, The Regulation of Premium Rate Services, was published in December 2004[54]. The report made a total of eighteen recommendations about how the range of problems surrounding the regulation of PRS could be addressed. These recommendations included, amongst others:

- Greater traffic monitoring and information sharing by telecoms companies
- Requirement that no monies should be paid out to service providers for at least 30 days after the charge was incurred
- Increased maximum fine which can be imposed by ICSTIS for breaches of the ICSTIS Code, and
- Improved provision for consumer refunds.

7.59 In addition, ICSTIS instituted a "prior permissions" regime for dialler software using premium rate numbers in August 2004. This aims to ensure that no network should provide numbers for diallers on premium rate numbers unless the service provider has a permission certificate from ICSTIS. The conditions which are attached to the certificate, which were in addition to the requirements of the ICSTIS Code, include:

- Terms and conditions of the service utilising the dialler must be clearly displayed on the users' screen, including costs per minute
- The user must confirm acceptance of the premium rate charge that will be incurred
- An on-screen clock must be made available by service provider which displays how many minutes the user has been connected to the dialler and/or cumulative costs accrued, and
- Dialler services are to be terminated by forced release after a cumulative call spend of £20.

7.60 ICSTIS' "prior permissions" regime covers most diallers using "09" numbers and those diallers which are supplied over numbers terminated outside the UK (international direct-dialled (IDD) numbers). It is important to note, however, that Ofcom does not have any powers in relation to IDD numbers. These are currently regulated through voluntary arrangements between ICSTIS and UK network operators, whereby UK network operators commit to shutting down links with overseas operators where there are clear breaches of the ICSTIS Code. As part of its

[54] See http://www.ofcom.org.uk/telecoms/ioi/nwbnd/prsindex/ntsprsdti/prs_review.pdf

"prior permissions" regime, ICSTIS received no applications from providers for permission to provide dialler services on these numbers, and therefore, diallers using IDD numbers are currently prohibited.

7.61 ICSTIS' "prior permissions" regime did not, however, encompass diallers using "08" numbers as Ofcom's PRS Condition, which requires service providers to comply with ICSTIS Code, did not include services where the charge or rate for the call is less than 10 pence per minute[55]. Instead, the PRS Condition covered only those services which are defined more narrowly as Controlled Premium Rate Services (CPRS), that is, PRS where the charge or rate for the call is more than 10 pence per minute. This meant that services using "08" numbers, for example those on "0871", did not have to comply with ICSTIS Code or with its "prior permissions" regime.

7.62 Taking advantage of this gap in regulatory provisions, many rogue diallers switched to using "08" numbers in an attempt to circumvent the requirement to obtain prior permission for service from ICSTIS. During 2005, there was growing evidence of consumer harm arising from rogue diallers using "08" numbers and, in particular, "087" numbers.

7.63 In order to address this gap, in 2005, Ofcom proposed to extend the definition of Controlled Premium Rate Services (CPRS), as set out in the PRS Condition, to include internet dialler software, irrespective of the call cost or number[56]. Pay-as-you-go dial up and unmetered dial up internet services – services provided by ISPs enabling narrowband access to the internet using a dial-up connection – were excluded from the proposed definition of internet dialler software for the purpose of the PRS Condition.

7.64 Following the consultation, in June 2006 Ofcom issued a statement on the PRS Condition confirming the strengthening of the PRS regulation to include internet dialler software irrespective of the telephone number used or the call charges involved[57]. All internet diallers have to comply with ICSTIS regulations, and, following the implementation period, will have to obtain prior permission from ICSTIS to provide the service.

International regulatory approaches

7.65 The problem of rogue internet diallers is not confined to UK consumers. During the early part of 2004, this issue rose in profile across Europe. Germany, for example, reported around 50,000 complaints in relation to diallers in 2004, while Switzerland was receiving around 300 complaints per month[58].

7.66 The problem has been addressed in different ways. Some countries, such as Germany, have passed specific regulations to make it illegal to download diallers without user consent. Like the UK, the countries that have adopted special regulations on diallers include Belgium, the Czech Republic, Finland and Spain.

7.67 Other countries have not taken specific legal measures, but have instead relied on preventive action taken by the ISPs on the basis of existing legislation against fraud.

[55] Chatline Services are automatically included under the PRS Condition regardless of the cost of call.
[56] Ofcom's consultation document is available for viewing on the Ofcom website at http://www.ofcom.org.uk/consult/condocs/prsconditions/prs.pdf
[57] The full document is available at http://www.ofcom.org.uk/consult/condocs/prsconditions2/
[58] The IRG Questionnaire on Modem Hijacking and Autodiallers, 2004

Additionally, some countries introduce barriers for dialling number ranges in uncommon country codes.

Case study – Germany

7.68 In Germany, internet diallers are allowed only for specific number ranges. All dialler service providers must be registered with the Federal Network Agency, the German regulatory authority responsible for electricity, gas, telecommunications, post and railway. In order to become registered, internet diallers have to meet certain minimum requirements. For example, users must be able to recognise diallers when they are installed and activated, and have to be able to disconnect them.

7.69 Additionally, the Federal Network Agency maintains a database of registered diallers, and their service providers, and makes it available to consumers on the regulator's website. All withdrawals of registered diallers as a result of breaches in service conditions are also published on the website so that users can be kept informed.

7.70 The Federal Network Agency does not carry out tests on diallers preventively, but when complaints arise, the litigated dialler is investigated. All offenders receive fines and can be punished by criminal law.

Conclusion

7.71 The evidence to date in the UK demonstrates that the measures taken have been largely effective in stamping out the abuse resulting from rogue diallers using premium rate numbering. The volume of complaints and enquiries received by ICSTIS about diallers using premium rate numbers during 2005 decreased substantially following the introduction of ICSTIS' prior permissions regime towards the end of 2004. The number of complaints received by ICSTIS regarding the use of "09" numbers fell from over 1,600 in January 2005 to around 300 in April 2006.

7.72 The increasing use of broadband access to the internet also works against this type of fraud because there is less dependency on dial-up access services which leave consumers more vulnerable to attacks.

7.73 However, the problem of rogue internet diallers is relatively new and many countries still have no established laws or procedures to tackle the problem. Where action has been taken recently, there is little evidence on how effective it has been in protecting consumers. This means that consumers in many countries are still vulnerable to harm as a result of rogue internet diallers.

Annex 1

Glossary of terms

Adware	Adware (a portmanteau of advertising-supported software) is any computer programme or software package, generally supplied free of charge, in which advertisements or other marketing material are included with, or automatically loaded by the software
Address	A string of characters that identify location, in the physical or network space e.g. your phone number, your postal home address. With respect to the Internet, it is the IP address assigned to an Internet host or an Internet session
ACMA	Australian Communications and Media Authority, the Australian converged communications regulator
AJAX	Asynchronous Javascript and XML is a term describing a web development technique for creating interactive web applications
APACS	Association for Payment Clearing Services. Set up in 1985 to oversee and manage payment clearing and money transmission services within the UK
APEC	Asia Pacific Economic Cooperation, established in 1989 to further enhance economic growth and prosperity for the region and to strengthen the Asia-Pacific community
APIG	All Party Internet Group, UK parliamentary group
APWG	Antiphishing Working Group, an international self-regulatory initiative to tackle fraud. APWG is a not-for-profit industry association whose members include financial institutions, online retailers, ISPs, the law enforcement community, security solutions providers and research institutions
ASA	Advertising Standards Authority
Backdoor	A loophole in a computer's security systems that allows a hacker to access or control it
Blog	Blog, truncated from weblog, is a web-based publication consisting primarily of periodic articles (normally in reverse chronological order). Although most early weblogs were difficult to update, tools to automate the running of such sites has made them accessible to a much larger population, and the use of some sort of browser-based interface is now a typical aspect of "blogging"
CATA	Canadian Advanced Technology Alliance
CRTC	Canadian Radio-Television and Telecommunications

	Commission, the Canadian communications regulator
CSA	Canadian Standards Association
Cookies	Cookies are small data files that a browser may store on the computer at the request of a web site server, designed to identify a user or a set of user preferences for a web site
Cybercrime	Cybercrime is a term used to describe criminal activity committed on the Internet
Dictionary Attack	A dictionary attack refers to the general technique of trying to guess a secret, typically a password by running through a list of likely possibilities, often a list of words from a dictionary
DNS	The Domain Name System is the directory of internet domain names. It is organized as a distributed database on the Internet. Specifically it ensures each fully qualified domain name has a unique IP address
Domain Name	A memorable name by which a host connected to the Internet is identified by internet users. Each domain name is uniquely associated with an IP address
DTI	Department of Trade and Industry, UK
EASA	European Advertising Standards Alliance, created in 1992 to demonstrate how the issues affecting advertising in the Single Market could be successfully dealt with through co-operation rather than detailed legislation
Encryption	Encryption is the process of obscuring information making it unreadable without the use of the decryption key
ENISA	European Network and Information Security Agency, created in 2004 to achieve a high and effective level of network and information security within the European Community
ETSI	European Telecommunications Standards Institute, which has the primary responsibility within Europe for the production of telecommunications standards for pan-European applications
Firewall	A security system consisting of a combination of hardware, software or a combination that limits the exposure of a host computer or a computer network to attack
FSA	Financial Services Authority, UK regulator for financial services
FTC	Federal Trade Commission, the US competition regulator
Grooming	In this context, grooming refers to actions deliberately undertaken with the aim of befriending a child in order to entice them into sexual activity
Hacking	Exploiting a system or gaining unauthorized access to the system

Host	Term used to refer to a computer connected to a network such as the Internet
Hosting	Storage of content and applications on servers connected to the network i.e. the Internet
HTML	HyperText Markup Language (HTML) is a standard markup language designed for the creation of web pages and other information viewable in a browser. HTML is used to structure information, for example denoting certain text as headings, paragraphs or lists
HTTP	HyperText Transfer Protocol is the standard protocol, used between end user web applications e.g. browsers and web servers, to request and transfer web content
HTTPS	HyperText Transfer Protocol Secure is the secure version of HTTP which uses certificates and encryption when sending data to prevent unauthorized interception and receipt of data. It is used for credit card payments and entry of sensitive personal or financial data
ICANN	Internet Corporation for Assigned Names and Numbers has overall responsibility for managing the DNS
ICRA	Internet Content Rating Association, an international body that encourages content providers to self-classify their content using ICRA's rating system
ICPEN	International Consumer Protection and Enforcement Network
Identity Theft	Refers to the unauthorised use of an individual's personal information in order to commit fraud or other crime
Interoperable	The features of systems which ensure interconnections provide reliable end-to-end service. Ability of a system to use elements of another system
Internet	A global network of networks, using a common set of standards (e.g. the Internet Protocol), accessed by users from a consumer device such as a computer, via a service provider
Internet Eavesdropping	Eavesdropping is the intercepting and reading of messages and conversations on the Internet by a third party
IP	Internet Protocol. The packet data protocol used for routing and carriage of messages across the Internet and similar networks
ISP	Internet Service Provider. A company that provides access to the Internet
ISPA	Internet Service Providers Association, UK trade association responsible for co-ordinating the ISP industry, particularly in relation to the protection of minors

ITU	International Telecommunications Union. A group of representatives from 161 countries headquartered in Geneva, Switzerland. The ITU publishes recommendations that influence telecom engineers, designers, manufacturers, and service providers around the world. These have the status of an international treaty and are binding on member states
IWF	Internet Watch Foundation, a UK based organisation which seeks to rid the Internet of illegal material such as child pornography
LIRs	Local Internet Registries are organizations that get allocated blocks of IP addresses from Regional Internet Registries, to assign and allocate to ISPs
Malware	Malware (a portmanteau of "malicious software") is any software programme designed to attack, degrade or prevent the intended use of a computer system or collect private data without the user's knowledge. Examples of malware include viruses, worms and trojans
OECD	Organisation for Economic Cooperation and Development was established in 1961, is an international agency which supports programmes designed to facilitate trade and development
OFT	Office of Fair Trading, UK's competition and consumer protection authority
Open Source Software	Open Source Software refers to software in which the source code is generally made available without charge to the wider developer community to study, modify and re-distribute under the software's governing licence terms
Peer-to-Peer	A method of communication in which two hosts or applications can initiate communications with each other and share resources without the need of an intermediate, central or master controller
Pharming	Pharming, a type of fraud that misdirects a browser to a malicious web site that impersonates a legitimate web site, typically through corrupting the DNS. Typically the user is deceived into divulging sensitive data such as a password or credit card number. Pharming, unlike Phishing, is beyond the control of the user, as the misdirection happens at the DNS level
Phishing	Phishing, a type of fraud that tricks users into visiting a malicious web site, typically though "spoofed" emails from well known banks, online retailers and credit card companies, where the user is deceived into divulging sensitive data such as a password or credit card number. Phishing can be prevented at the user level, unlike pharming
Pop-up adverts	A form of online advertising on the web where an advertisement appears in a separate window on top of the current window
PKI	Public Key Infrastructure is a standardised system for the secure exchange of electronic signatures and identification for use on the

	Internet
Protocol	A “set of rules” that define an exact format for communication between two end systems. For example the HTTP protocol defines the format for communication between web browsers and web servers
Registrar	A business or organization accredited by ICANN that has the ability to register domain names on the behalf of entities interested in holding a domain name
RIRs	Regional Internet Registries is an organization that oversees the registration and allocation of IP addresses to Local Internet Registries in a region for example, the Réseaux IP Européens (RIPE) Network Coordination Centre is Europe’s RIR
RIPE NCC	Réseaux IP Européens Network Coordination Centre is one of five global regional Internet registries, responsible for overseeing and allocating IP addresses to local internet registries in Europe
Session	An unbroken period of time during which a connection is maintained between two systems or applications
SMTP	Simple Mail Transfer Protocol (SMTP) is the de facto standard protocol for email communication across the Internet
SPAM	Unsolicited commercial email sent to a large number of addresses
Spyware	Software installed on an individual’s computer which covertly transmits information about the user’s activities to a remote host
Standards	A definition or format that has been approved by a recognised standards organization or is accepted as a de facto standard by the industry. Standards exist for programming languages, operating systems, data formats, communications protocols, and electrical interfaces
Tags	A sequence of characters in a markup language like HTML, used to provide information, such as formatting specifications, about a particular element
Tier	Class or rank
Trojan	A type of malware, a malicious programme which appears as a benign application
TWF	Television Without Frontiers, an EU directive governing the conditions that a broadcaster needs to comply with to operate in the EU. It is currently under review
Virus	A type of malware; an unwanted, disruptive, and sometimes destructive programme that hides within another seemingly innocuous programme, and produces copies of itself which it

	inserts into other programmes or documents
VGT	Virtual Global Taskforce is made up of law enforcement agencies from around the world, working together to fight child abuse online
VoIP	Voice over Internet Protocol. A technology that allows users make telephone calls, either over the public Internet or over private IP networks
UNCITRAL	United Nations Commission on Trade Law
WARC	World Administrative Radio Conference sponsored by the ITU
Worms	A type of malware, which replicates itself and is self-propagating. Unlike a virus it does not attempt to conceal itself in other programmes, but is a stand-alone programme
Web	Short for World Wide Web (WWW), the vast collection of online content accessible through the Internet, viewed through a browser, and interconnected by hypertext links
XML	eXtended Markup Language is a standard markup language like HTML but is more flexible and extendible