



# Ofcom response to the Lords Science and Technology Committee report on Personal Internet Security

Ofcom welcomes the opportunity to respond to the recommendations of the Lords Science and Technology Committee. The Committee has undertaken a wide-ranging review of the risks consumers face when they use and participate in services offered on the internet. From Ofcom's viewpoint the questions they have raised around issues of personal internet security form part of a more general debate around the risks consumers face as they engage with the internet, spanning:

- The risks of harm which may arise from the exposure of children to inappropriate content
- The risks from virus and other attacks on consumers' PCs, which can lead to loss of data or to the PC being exploited for illegal purposes (e.g. sending spam)
- The risks of fraud or identity theft which may arise as a result of the purchasing of products and services online, or from sharing personal information online, for example on social networking sites

These are significant issues for consumers, and require attention from industry, Government and regulators. Ofcom's own research suggests that around 20% of consumers have top of mind concerns about their internet service. The highest ranked spontaneous concerns relate to the type of material available online (e.g. sex/violence/adult material (6%)) and internet security (6%). When prompted, the proportion of consumers with concerns about their internet service rises to around 80%, and the highest ranked concerns are for children accessing adult content via the internet and issues around personal identity theft.

The Committee's inquiry and recommendations focus on personal security, but some of the questions raised are common to the full range of internet issues. Most importantly, there is a question over the locus of responsibility for these risks - who has the duty to protect consumers.

The Committee's suggestion that this is a distributed duty is one with which Ofcom agrees. Some degree of responsibility will remain with the consumer, and many of the Committees' recommendations - such as the support for Get Safe Online - are intended to enhance consumers' ability to protect themselves. Ofcom's own Media Literacy work programme, outlined below, is focused substantially on helping consumers protect themselves (primarily in relation to harmful content risks).

Like the Committee, Ofcom does not believe that responsibility lies exclusively with the consumer: industry players equally have an essential contribution to make to personal internet security. At least in relation to security issues, ISPs in particular can play an important role, and the Committee received some evidence of the efforts that the more responsible ISPs already make in this area.

As the authority responsible for overseeing the wholesale and retail markets for internet connectivity, we have a clear interest in those aspects of the review which focus on the role that ISPs play in personal security. Ofcom believes that the ISP contribution to security could have a greater impact than at present. For example, security could be a more important feature of the service provided, and there could be greater transparency about the security support which consumers can expect, and which ISPs should provide.

Ofcom has engaged with the Internet Service Providers' Association (ISPA), the ISP trade body, with a view to exploring what more the industry could do to address subscribers' security needs. The first phase of this engagement is some research to understand exactly what the extent is of ISPs security support today – for example, the proportion of ISPs which offer spam filtering or firewall software as part of the basic subscription package, and the extent of consumer take-up of these services.

There is a second, fundamental question common to the issues identified above – whether ISPs should have regulatory duties, either in relation to harmful content or to the security risks the Committee has explored. This question has already been debated both at UK and EU level – and EU and UK legislation (for example the Communications Act 2003, the E-Commerce Directive and the General Authorisation Directive) currently preclude Ofcom from acting to impose content or security duties in relation to internet services.

Nonetheless, as the Committee's report implies, it may be appropriate to re-examine this fundamental question, something we expect the UK will be able to do as part of the debates over the Electronic Communications Framework, and the E-Commerce Directive happening in the EU over the next 2-3 years.

As well as introducing these broad themes, the Committee makes specific recommendations for Ofcom in relation to its media literacy duties, its regulation of Voice Over Internet Protocol (VOIP) service providers, and in relation to the

development of a number of British Standards Institute Kitemarks, and on which we comment below.

In order to put into context Ofcom's response to the issues raised by the Committee, we must give a brief account of our Media Literacy work programme. We do so below, and then deal directly with the relevant recommendations from the Committee:

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 and the processes and systems by which this is delivered, regulated and controlled.

Ofcom defines media literacy as the ability to access, understand and create communications in a variety of contexts. Without media literacy skills, people's ability to participate effectively in society may be greatly diminished.

Ofcom's Media Literacy strategy was set out in a Statement published on 2 November 2004<sup>1</sup>.

Ofcom's work to promote Media Literacy is intended:

- to give people the opportunity and motivation to develop competence and confidence to participate in communications technology and the digital society
- to inform and empower people to manage their own media activity (both consumption and creation).

---

<sup>1</sup> [http://www.ofcom.org.uk/consult/condocs/strategymedialit/ml\\_statement/](http://www.ofcom.org.uk/consult/condocs/strategymedialit/ml_statement/)

## Ofcom's Response to Specific Committee Recommendations

### **Recommendation 8.23**

We further recommend that, in addition to the new kite mark for content control software, Ofcom work with industry partners and the British Standards Institute to develop additional kite marks for security software and social networking sites; and that it continue to keep under review possible areas where codes of best practice, backed up by the kite marks, might be appropriate. (6.48)

We welcome the Committee's interest in the pioneering work to create a kite mark<sup>2</sup> as a way of raising the effectiveness and ease of use of these software tools. Once the Standard for the content control software is published and kite marks awarded we will carefully monitor the impact of them on the take-up and use of the products. If, as we hope, they prove an effective way of encouraging the use of content control software we will encourage industry to extend the scheme to internet security tools.

Given the fast pace of change in the online environment, the Committee has rightly pointed out the need for continual examination of the online environment for areas where codes of best practice might be appropriate. Ofcom believes that it can best play a role in developing such best practice guidance through its ongoing support for the Home Office Task Force for Child Protection on the Internet.

The Home Office Task Force for Child Protection on the Internet, comprising representatives from Government, industry and the child protection charities, was convened to consider how to make the internet the safest place for children. This established forum of key stakeholders has delivered significant progress in encouraging effective action to improve practice in moderation of chatrooms, instant messaging and in providing safe internet search engines. They have established a number of best practice guides, with the support of industry, and continue to monitor

---

<sup>2</sup> The Home Office, Ofcom's Media Literacy team, service providers and software developers have been working for the past two years to develop the kite mark for content control software mentioned in this recommendation (a British Standard for Internet Access Control Software (PAS 74)). The Standard aims to allow UK adult internet users to easily control children's access to inappropriate internet-based content and services. Products meeting the requirements of the specification will be entitled to display a Kite mark on promotional materials and packaging to help consumers identify products which are both effective and easy to use.

issues which might warrant the creation of best practice guides in the future. The latest guidance for Social Network providers is due to be published later this year.

In line with the Committee's thinking, Ofcom believes that it is timely to review the implementation of the Mobile Content Code. In collaboration with the Home Office, the Children's Charities Coalition on Internet Safety (CHIS), and industry Ofcom has launched a project to review how the Codes are being used by industry and how effective they are in protecting people from exposure to unwanted material. This evaluation will help update the Codes and direct future activity in this area.

**Recommendation 8.24**

We recommend that the Department for Children, Schools and Families, in recognition of its revised remit, establish a project, involving a wide range of partners, to identify and promote new ways to educate the adult population, in particular parents, in online security safety. (6.49)

We recognise that adults often lack confidence and competence in the use of technology and that they often devolve these tasks to younger members of the family. Ofcom has, for the last three years supported the various adult learning campaigns across the UK as part of Adult Learners' Week. We look forward to working with the DCSF and other agencies on initiatives aimed at promoting the media literacy of adults.

**Recommendation 8.22**

We recommend that Ofcom not only co-sponsor the Get Safe Online project, but that it take responsibility for securing support from the communications industry for the initiative. (6.47)

We welcome the significant achievement of all stakeholders in the development and launch of the Get Safe Online (GSO) campaign. Ofcom supports the need to provide people with information on the potential threats from using the internet. GSO is an important initiative which should receive adequate funding. Given the extensive work undertaken by GSO in this area and since both GSO and Ofcom's Media Literacy work are funded by central government, Ofcom has focused its resources in other areas. (Total funding from Government for Ofcom's media literacy function was £559,000 last year). Ofcom will, however, explore with GSO ways in which we might encourage industry to support the GSO campaign.

Personal internet security is an important issue and is included in Ofcom's media literacy research and in our future planned activity. We have commissioned further research into people's usage and attitudes to media and have included questions related to people's safety and security online. The findings of this research will be published early in 2008 and this will guide both Ofcom's and the industry's activity to promote safer internet use.

#### **Recommendation 8.11**

The uncertainty over the regulatory framework for VOIP providers, particularly with regard to emergency services, is impeding the development of this industry. We see no benefit in obliging VOIP providers to comply with a regulatory framework shaped with copper-based telephony in mind. We recommend instead that VoIP providers be encouraged to provide a 999 service on a "best efforts" basis reflecting the reality of internet traffic, provided that they also make clear to customers the limitations of their service and the possibility that it may not always work when it is needed. (3.70)

In its oversight of the VOIP sector, Ofcom has sought to provide clarity and certainty for operators. The Committee is correct in suggesting that the complete regulatory framework which applies to copper-based telephony should not be generally applied to VOIP. It is for this reason that, for example, Ofcom's 2006 Consultation<sup>3</sup> and March 2007 Statement<sup>4</sup> on VoIP regulation, recognised that existing guidelines on complying with network integrity requirements (the *Essential Requirements Guidelines*<sup>5</sup>) were suited to traditional PSTN providers and not VoIP providers

Currently, all VOIP providers operate under a Code of Practice, the *Code on the provision by Service Providers of consumer information to Domestic and Small Business Customers for the provision of Services*. The Code requires VoIP providers to provide customers with information about any feature or limitation that differs from a standard phone service provided over the PSTN, in particular the availability or standard of 999 access. This is broadly consistent the Committee's recommendation.

<sup>3</sup> *Regulation of VoIP Services*, 22 February 2006

<http://www.ofcom.org.uk/consult/condocs/voipregulation/>

<sup>4</sup> *Statement on the Regulation of VoIP Services*, Ofcom, 29 March 2007

<http://www.ofcom.org.uk/consult/condocs/voipregulation/voipstatement/voipstatement.pdf>

<sup>5</sup> *Guidelines on the essential requirements for network security and integrity*, Ofcom, 9 October 2002

[http://www.ofcom.org.uk/static/archive/oftel/publications/ind\\_guidelines/guid1002.htm](http://www.ofcom.org.uk/static/archive/oftel/publications/ind_guidelines/guid1002.htm)

However, there is a broad range of forms which VOIP services may take, and Ofcom's regulatory approach to VOIP must take account of these different forms. In particular, Ofcom must take account of the extent to which particular types of VOIP will substitute for traditional PSTN telephony services, given that consumers have well established expectations of their PSTN service, which include an expectation of 999 access.

In its most recent consultation on the issue, issued in July 2007, Ofcom proposed that those VOIP services which allow outgoing telephone calls to be made over the internet to the Public Switched Telephony Network (PSTN), should provide access to the emergency services. The consultation closed on the 20<sup>th</sup> September.

This proposal is based on a range of evidence, most notable among which are the facts that domestic VOIP use doubled to 10% of households over the year to Q4 2006; that two thirds of consumers with VOIP have a service without 999 access; and that of those almost 80% thought the service offered 999 access or were unaware that it did not<sup>6</sup>.

Ofcom therefore considers the information requirements in the current Code to be important but not sufficient. Ofcom's Impact Assessment demonstrates that the benefits of lives saved by requiring VoIP services to offer 999 access would significantly outweigh the costs of compliance.

In the consultation, Ofcom invites responses on the current means, future possibilities and limitations for providing network integrity, service reliability and caller location information, in the event that Ofcom's proposal is adopted.

If implemented, Ofcom would enforce, monitor and review its policy to ensure VoIP providers are compliant and to see if our regulations need to be adapted for VoIP providers.

For further information, please see the Ofcom consultation *Regulation of VoIP Services: Access to the Emergency Services*, 26 July 2007, at <http://www.ofcom.org.uk/consult/condocs/voip/>

---

<sup>6</sup> Ofcom *Research Report: Voice over Internet Protocol (VoIP)*, [www.ofcom.org.uk](http://www.ofcom.org.uk).

