House of Commons

Culture, Media and Sport Committee

Harmful content on the Internet and in video games

Tenth Report of Session 2007–08

Volume I

Report, together with formal minutes, oral and written evidence

Ordered by The House of Commons
to be printed 22 July 2008

HC 353-I
Published on 31 July 2008
by authority of the House of Commons
London: The Stationery Office Limited
£0.00

The Culture, Media and Sport Committee

The Culture, Media and Sport Committee is appointed by the House of Commons to examine the expenditure, administration, and policy of the Department for Culture, Media and Sport and its associated public bodies.

Current membership

Mr John Whittingdale MP (*Conservative, Maldon and East Chelmsford*) *[Chairman]*
Janet Anderson MP (*Labour, Rossendale and Darwen*)
Mr Philip Davies MP (*Conservative, Shipley*)
Mr Nigel Evans MP (*Conservative, Ribble Valley*)
Paul Farrelly MP (*Labour, Newcastle-under-Lyme*)
Mr Mike Hall MP (*Labour, Weaver Vale*)
Alan Keen MP (*Labour, Feltham and Heston*)
Rosemary McKenna MP (*Labour, Cumbernauld, Kilsyth and Kirkintilloch East*)
Adam Price MP (*Plaid Cymru, Carmarthen East and Dinefwr*)
Mr Adrian Sanders MP (*Liberal Democrat, Torbay*)
Helen Southworth MP (*Labour, Warrington South*)

Powers

The Committee is one of the departmental select committees, the powers of which are set out in House of Commons Standing Orders, principally in SO No 152. These are available on the Internet via www.parliament.uk.

Publications

The Reports and evidence of the Committee are published by The Stationery Office by Order of the House. All publications of the Committee (including press notices) are on the Internet at

http://www.parliament.uk/parliamentary_committees/culture__media_and_sport.cfm

Committee staff

The current staff of the Committee are Kenneth Fox (Clerk), Martin Gaunt (Second Clerk), Anna Watkins/Lisa Wrobel (Committee Assistants), Rowena Macdonald (Secretary), Jim Hudson (Senior Office Clerk) and Laura Humble (Media Officer).

Contacts

All correspondence should be addressed to the Clerk of the Culture, Media and Sport Committee, House of Commons, 7 Millbank, London SW1P 3JA. The telephone number for general enquiries is 020 7219 6188; fax 020 7219 2031; the Committee's email address is cmscom@parliament.uk

Contents

Report

Summary

More and more, the Internet is becoming a part of our lives. For communications, research and commerce, it is now an indispensable tool. However, anyone who regularly watches television or reads the press is likely to have become aware of growing public concern in recent months at the Internet's dark side, where hardcore pornography and videos of fights, bullying or alleged rape can be found, as can websites promoting extreme diets, self-harm, and even suicide.

There is particular anxiety about the use of social networking sites and chatrooms for grooming and sexual predation. Although these environments may appear to a child to be relatively private, with defined boundaries, in fact a user's profile or an online forum may be open to thousands or even millions of other users, all able to view even if they do not actively participate. Unless a user of a networking site takes steps to control access to their territory, he or she is potentially exposed to malicious communication or comment and invasions of privacy.

There is heated debate about whether certain types of content cause harm, particularly to children, and whether there is a direct link between exposure to violent content on the Internet or in video games and subsequent violent behaviour. The conclusion overall is that there is still no clear evidence of a causal link; but incontrovertible evidence of harm is not necessarily required in order to justify a restriction of access to certain types of content in any medium, and we conclude that any approach to the protection of children from online dangers should be based on the probability of risk.

We welcome the analysis by Dr Byron of the risks posed by the Internet to children and agree with her conclusion that a UK Council for Child Internet Safety should be established. We are concerned at reports from some key players that there has been little opportunity to influence decisions as to how the Council will operate in practice.

Sites which host user-generated content—typically photos and videos uploaded by members of the public—have taken some steps to set minimum standards for that content. They could and should do more. We recommend that terms and conditions which guide consumers on the types of content which are acceptable on a site should be prominent. It should be made more difficult for users to avoid seeing and reading the conditions of use: it would then become more difficult for users to claim ignorance of terms and conditions if they upload inappropriate content.

It is not standard practice for staff employed by social networking sites or video-sharing sites to preview content before it can be viewed by consumers. Some firms do not even undertake routine review of material uploaded, claiming that the volumes involved make it impractical. We were not persuaded by this argument, and we recommend that proactive review of content should be standard practice for sites hosting user-generated content. We look to the proposed UK Council to give a high priority to reconciling the conflicting claims about the practicality and effectiveness of using staff and technological tools to screen and take down material. We also invite the Council to help develop agreed standards across the Internet industry on take-down times—to be widely publicised—in

order to increase consumer confidence.

It is common for social networking sites and sites hosting user-generated content to provide facilities to report abuse or unwelcome behaviour; but few provide a direct reporting facility to law enforcement agencies. We believe that high profile facilities with simple, preferably one-click mechanisms for reporting directly to law enforcement and support organisations are an essential feature of a safe networking site. We would expect providers of all Internet services based upon user participation to move towards these standards without delay.

The designation of some of the more extreme types of material as illegal has had a beneficial effect in restricting the amount of harmful content hosted in the UK and in limiting access to harmful content hosted abroad. We do, however, believe that the UK Council for Child Internet Safety should discuss with the Ministry of Justice whether the law on assisted suicide is clear enough to enable not just successful prosecutions but also action to block access to websites which assist or encourage suicide.

As things stand, companies in the Internet industry largely regulate themselves. We believe that self-regulation has a range of strengths: a self-regulating industry is better placed to respond quickly to new services; it is more likely to secure "buy in" to principles; and it will bear the immediate cost. We accept that significant progress has been achieved through self-regulation by the various industries offering Internet-based services, but there appears to be a lack of consistency and transparency of practice, and the public needs the assurance that certain basic standards will be met. Rather than leap to statutory regulation, we propose a tighter form of self-regulation, under which the industry would speedily establish a self-regulatory body to draw up agreed minimum standards based upon the recommendations of the UK Council for Child Internet Safety, monitor their effectiveness, publish performance statistics, and adjudicate on complaints. In time, the new body might also take on the task of setting rules governing practice in other areas such as online piracy and peer to peer file-sharing, and targeted or so-called "behavioural" advertising.

Several Government departments have an interest in this field, and it does seem that there is scope for improved co-ordination of activity between them. A single Minister should have responsibility for co-ordinating the Government's effort in improving levels of protection from harm from the Internet, overseeing complementary initiatives led by different Government departments, and monitoring the resourcing of relevant Government-funded bodies.

There is a distinct issue about labelling of video games to indicate the nature of their content. Two systems currently exist side by side: the industry awards its own ratings, and the British Board of Film Classification awards classifications to a small number of games which feature content unsuitable for children. The dual system is confusing, and Dr Byron recommended that there should instead be a single hybrid system. We believe that Dr Byron's solution may not command confidence in the games industry and would not provide significantly greater clarity for consumers. While either of the systems operated by the BBFC and by the industry would be workable in principle, we believe that the widespread recognition of the BBFC's classification categories and their statutory backing offer significant advantages which the industry's system lacks. We therefore agree that the BBFC should have responsibility for rating games with content appropriate for adults or

teenagers, as proposed by Dr Byron, and that these ratings should appear prominently. Distributors would of course be free to continue to use industry ratings in addition.

1 Introduction

1. More and more, the Internet is becoming a part of our lives. For communications, research and commerce, it is now an indispensable tool. Governments are right to attach high priority to ensuring that all citizens have access to broadband delivery and are able to take full advantage of all it has to offer. However, anyone who regularly watches television or reads the press is likely to have become aware of growing public concern in recent months at the Internet's dark side: the easy availability of hardcore pornography, which people may find offensive, the uploading by ordinary people of film of real fights, bullying or alleged rape, or the setting up of websites encouraging others to follow extreme diets, or self-harm, or even commit suicide. In particular, there is increasing anxiety among parents about the use of social networking sites and chatrooms for grooming and sexual predation.[1]

2. In March 2007, the Rt. Hon. Gordon Brown MP gave a speech to the Equal Opportunities Commission, in which he spoke about parents' wishes for their children and how they could be fulfilled. He said that "we want to promote a culture which favours responsibility and establishes boundaries" and that "we need to harness new technology and use it to enable parents to exercise the control they want over the new influences on their children"; he went on to say that he had discussed with Ofcom further measures to protect children from unsuitable material in the media. He said that Ofcom would:

- Conduct an information campaign for parents which will let them know what parental control software is available for computers and TV set-top boxes;
- Work with equipment manufacturers to ensure parents have better information on how to use blocking software;
- Consider what more can be done to assist parents in restricting access to violent and obscene material sent over the internet; and
- Work with the Internet Watch Foundation to ensure that internet service providers tell their subscribers about software which blocks access to sites.

3. This initiative was largely overtaken, however, in September 2007, when the Prime Minister, the Secretary of State for Children, Schools and Families and the Secretary of State for Culture, Media and Sport announced that a review was to be set up to examine ways of helping children and parents "get the best" from new technologies while protecting them from harmful images. The review was to be led by Dr Tanya Byron, a clinical psychologist.[2] The objectives of the review were:

- To undertake a review of the evidence on risks to children's safety and wellbeing of exposure to potentially harmful or inappropriate material on the internet and in video games; and

[1] *BBC Panorama* has broadcast two programmes exploring this theme, one about film of brutal fights between children (30 June 2007) and another about the use of social networking sites to groom children (7 January 2008)

[2] DCSF Press Release 6 September 2007

- To assess the effectiveness and adequacy of existing measures to help prevent children from being exposed to such material, to help parents understand and manage the risks of access to inappropriate content, and to make recommendations for improvements or additional action.

4. Dr Byron's report was published on 27 March 2008, and the Government announced on the day of publication that it accepted in full all of her recommendations, albeit with public consultation in one area.[3] Dr Byron's review was thoughtful and thorough and the report is in many ways a highly impressive piece of work.

5. The terms of reference for our inquiry were announced in December 2007 and were more widely drawn:

— The benefits and opportunities offered to consumers, including children and young people, and the economy by technologies such as the Internet, video games and mobile phones;

— The potential risks to consumers, including children and young people, from exposure to harmful content on the Internet or in video games. The Committee is particularly interested in the potential risks posed by:

  - "Cyber bullying";
  - user generated content, including content that glorifies guns and gang violence;
  - the availability of personal information on social networking sites;
  - content that incites racial hatred, extremism or terrorism;
  - content that exhibits extreme pornography or violence;

— The tools available to consumers and industry to protect people from potentially harmful content on the Internet and in video games; and

— The effectiveness of the existing regulatory regime in helping to manage the potential risks from harmful content on the Internet and in video games.

6. We have not examined the use of the Internet to perpetrate fraud through false claims, phishing or other means. Nor have we attempted to consider the issues raised by Dr Byron in the same depth. Our inquiry has, however, served as a sounding board for responses to Dr Byron's recommendations, and this Report gives views on matters which she raised and which have provoked particular debate. In some areas, its scope is also wider than hers and does not focus on threats to children alone. Our aim is to feed into the process for implementation of Dr Byron's recommendations and to identify other areas worthy of attention. As is our usual practice, we are publishing most of the written submissions to our inquiry alongside the oral evidence.

7. During the inquiry we visited the Child Exploitation and Online Protection Centre in London; and we travelled to the United States for meetings with providers of social

[3] Classification of video games: see paragraph 7.50 of the Byron Review

networking services and search services, and with video games publishers. We are grateful to our hosts both in the UK and in the US for sharing their views. We also record our thanks to our Specialist Adviser, Mr Ray Gallagher, who has provided advice on a range of matters concerning broadcasting and new media.

2 Opportunity

8. This inquiry flows directly from the growth of the Internet into a mass medium for communication, and distribution of creative content. The Internet is no longer simply a resource for information and research and a path for e-mail traffic: it has become an interactive social forum, a means for supplying entertainment, a way of allowing people to work more flexibly and a tool which many use almost daily to manage finances and to buy goods and services. It has provided new scope for people to air their views freely and openly. While the benefits have increased, however, so have attendant risks. The Internet is a public space, something which may not be readily apparent, particularly to children; and this inquiry has explored ways in which the inherent risks might be managed.

9. The last three years have seen exponential growth in the use of the Internet to transmit creative content. Audio-visual material from a vast range of providers, including programming from traditional broadcasters, is available on the Internet. In addition, films, music, games and images can all be downloaded with ever greater ease as broadband speeds increase. We considered the impact of some of these developments in detail in our Report on New Media and the Creative Industries.[4]

10. Underlying the use of the Internet for the transmission of creative content is the widespread availability of broadband and the faster connection times offered. The Government told us that 99.8% of households are now able to access broadband,[5] and 88.4% of all Internet connections in September 2007 used broadband.[6] Digital files containing audio-visual material are large and, in practice, can only be distributed using the higher connection speeds available through broadband. 49.2% of all Internet connections in September 2007 had a speed greater than 2Mbps, compared to 35.5% of connections in December 2006.[7]

[4] Fifth Report of Session 2006-07, HC 509-I

[5] Ev 342

[6] Office for National Statistics 20 November 2007

[7] Office for National Statistics 20 November 2007

11. Research by Ofcom published in 2007 indicated that 99% of children accessed the Internet, most often at home and at school:

	Any access : 8-17 year olds	Most often access: 8-17 year olds
PC/laptop at home	81%	65%
School/college	86%	26%
Library	12%	1%
Internet cafe	3%	
Friend's house	23%	2%
Relative's house	11%	2%
Mobile phone	7%	1%
Any internet use	99%	
Don't use the internet	1%	
Use internet but not at home	18%	

Source: Ofcom – Children, Young People & Online Content, October 2007; survey base of 513 children aged between 8 and 17

12. Along with the faster broadband speeds which are now becoming more widely available, the Internet is more and more frequently being accessed by devices other than computers, such as mobile telephones, iPods, personal digital assistants (PDAs) and games consoles. All allow access "on the move" and, for children, free from parental supervision. O_2 cited figures showing that 50% of 10 year olds and 90% of 12 year olds have mobile phones.[8] The Children's Charities' Coalition for Internet Safety (CHIS), in its response to the Byron Review, referred to research by Childwise[9] suggesting that 96% of children in the UK had access to mobile phones by the age of 11 and that "more or less a third" were using mobile devices to access the Internet.[10]

13. The appeal of access through portable devices is likely to grow as the range of devices increases. The Internet Watch Foundation told us that, in Japan, there was more access to the Internet via mobile technologies than from fixed access points and that there was "every reason to think that this trend will apply to the UK as more and more portable electronic devices come on stream".[11] T-Mobile told us that consumers valued the ability to generate their own content and update their personal social networks wherever and

[8] Carphone Warehouse Mobile Youth Report 2006, Ev 66

[9] A market research agency specialising in research concerning children

[10] Ev 8

[11] Ev 45

whenever they choose.[12] Mr Bartholomew, Head of Public Affairs at O_2, described the Internet access facility on the iPod touch and the iPhone as "fantastic" and "like having a computer with a smaller screen".[13]

Social networking and video-sharing websites

14. For the purposes of this inquiry, perhaps the most significant development of the last two or three years has been the growth in social networking and the ease with which users can upload and share content, principally images, comment and videos. A great deal of this content is created by users themselves, hence the term "user-generated content". This "new generation" Internet is frequently termed Web 2.0: Google told us that whereas Web 1.0 "was characterised by static websites, download of content, limited use of search engines and surfing from one website to another", Web 2.0 "represents a fundamental shift away from this model, towards a more dynamic and interactive Internet where content is generated by users, uploaded by others and enjoyed within online communities".[14]

15. In 2005, the concept of a social networking website was largely unknown. In the last two years, there has been an explosion in the number of users of such sites to converse online with friends. Orange told us that participation in the UK in social networking sites was the highest in Europe, with 24.9 million unique[15] visitors, amounting to 78% of the total online population in the UK.[16] T-Mobile told us that social networking and interactive sites were at the forefront of driving mobile phone usage: eight out of the twenty websites most frequently visited using mobile devices are social networking sites.[17]

16. Bebo, a social networking site popular in the UK and targeted at people aged under 30, told us that social networking sites have strong benefits and that Web 2.0 services (i.e. those based upon sharing of material among online communities and dissemination of user-generated content) offered enormous creative opportunities, not least through citizen journalism, as well as providing a forum for developing digital literacy and the ability to express yourself online and to make "informed choices". Bebo suggested that such services created "social capital" and filled a vacuum in community engagement.[18] MySpace argued that social networking performed an important function in the sociological development of young people, assisting them in forming an adult identity and expressing themselves.[19]

17. Some sites are designed purely to host images and videos. Flickr, launched in 2004, was one of the first sites to become prominent in the UK; between 3 million and 5 million photos are understood to be uploaded to Flickr daily.[20] Other sites include YouTube, which describes itself as "a leading video hosting site and the premier destination to watch and

---

[12] Ev 60

[13] Q 136

[14] Ev 116

[15] A "unique visitor" is a unit of traffic to a website, in which each visitor is counted only once in a given timeframe

[16] Ev 69

[17] Ev 60 and 61

[18] Ev 144

[19] Q 383

[20] www.techcrunch.com 13 November 2007

share original videos worldwide".[21] Approximately ten hours' worth of content is uploaded to YouTube every minute.[22]

18. The popular appeal and astonishing growth of YouTube and other such sites has made them assets worth acquiring at a time of industry consolidation. Flickr was acquired by Yahoo! in March 2005; YouTube was acquired by Google in autumn 2006 for $1.65 billion; and Bebo was acquired by AOL in March 2008 for $850 million. We note that one social networking website, even though it does not currently attract large advertising volumes, has been valued at up to $15 billion—Facebook.[23]

Video games

19. The intricacy of video games now available on DVD and via the Internet is in stark contrast to the primitive games (such as Space Invaders and Pacman) which marked the birth of the genre. Games can be played on dedicated games consoles, personal computers (PCs) and other devices; they have highly realistic graphics and are now labyrinthine in their complexity, offering many levels of play and options within each game. According to the Government's written submission, 59% of the UK population play video games, the average age of gamers is 28, and one in four women play video games.[24] We understand from ELSPA that one in three men plays video games.[25]

20. Increasingly, games are played online, with players competing against others in real time. Online games may be constantly updated, with new features being introduced by games publishers. Some games, known as MMORGs (Massively Multiplayer Online Roleplaying Games), are virtual worlds with possibly thousands of gamers logged in from separate computers or games consoles, each assuming the role of a fictional character, often playing a role or undertaking a quest or activity which can unfold over a series of weeks. The industry forecasts that online gaming will, in time, overtake downloadable or hard-copy games.[26]

21. The UK has a thriving video games industry. According to ELSPA (the Entertainment and Leisure Software Publishers Association), approximately 35% of software sold in Europe emanates from creative studios in the UK; and the UK industry employs around 22,000 people and attracts significant inward investment from the US and Japan.[27] Until recently, the UK's position in the games industry (in terms of revenue generated) was second only to that of the US and Japan, generating sales in excess of £2.3 billion in 2006";[28] the UK has now been displaced into fourth place by Canada, which offers significant tax concessions to stimulate the industry locally.[29] Despite this, witnesses from ELSPA

[21] Ev 115

[22] Q 313

[23] Ev 281

[24] Ev 342

[25] Information supplied by the Entertainment and Leisure Software Publishers Association (ELSPA)

[26] Q 462

[27] Ev 164

[28] Ev 164

[29] Q 627

(representing games publishers) and TIGA (representing games developers) described the outlook as "very positive" and believed that the industry was set to grow.[30]

22. Various witnesses stressed the potential benefits of games. Mr Carrick-Davies, Chief Executive of Childnet International, told us that playing video games "improves children's confidence, their sense of social standing [and] their ability to multi-task".[31] The Government gave examples of how games had been used in curriculum-based learning and training of the military in communications and decision-making skills; and it said that video games could engage and motivate learners, including those disaffected or previously hard to reach.[32] Tiga (a trade body for games developers) also pointed out that so-called "serious games" are being researched for possible use in military, educational, health and training applications.[33] The Interactive Software Federation of Europe noted that video games can provide a "playful way to hone IT skills".[34]

23. Dr Byron, in her report, acknowledged that there are potential educational benefits to some video games, particularly in terms of motivating pupils, but she argued that these should not be overstated: "Most researchers and certainly educationalists would argue that using a video game…to aid learning is not in itself the key to success. It is the context around the child and the technology (i.e. the skills of the teacher) that determines whether it becomes a successful learning experience".[35] Professor Livingstone, who jointly undertook on behalf of Ofcom a review of research into potential harmful content, also questioned the strength of evidence that playing video games benefited children.[36]

Virtual worlds

24. One of the best-known examples of a virtual forum is *Second Life*, a three-dimensional "world" in which participants can assume a virtual persona (or "avatar"), meet and communicate with others, create "anything you can imagine", trade virtual goods on a virtual exchange, acquire virtual "land" and build upon it.[37] The Government told us that virtual worlds offered benefits to both the consumer and to public and private sector organisations: it observed that the National Physical Laboratory had been using *Second Life* for scientific knowledge transfer with colleagues in NASA, and that universities and other bodies were piloting the use of *Second Life* for use in healthcare and other fields of research.[38]

---

[30] Q 452

[31] Q 3. See also Microsoft Ev 32

[32] Ev 343

[33] Ev 163

[34] Ev 386

[35] *Byron Review*, page 155

[36] Professor Sonia Livingstone Q3

[37] See secondlife.com

[38] Ev 343

3 Types of risk

25. The ease of communication, the ready availability of creative and informative content and the global reach which are all such powerful features of the Internet, are of huge benefit. In each case, however, those strengths have flipsides: malicious communication is as easy as benign communication, content may be potentially harmful or illegal, and global reach allows access from almost anywhere in the world to content which would be illegal in one's home country.

26. Social networking sites and chatrooms are new types of environment which may appear to a user to be relatively private, with defined boundaries, when in fact a user's profile or an online forum may be open to thousands or even millions of other users, all able to view even if they do not actively participate. Some users of social networking sites may choose to limit the visibility of their "profiles" but many do not: their profile page then becomes a public space. Many users, particularly children, are not even aware that their personal information is being made available to anyone who chooses to access it. Unless a user of a networking site takes steps to control access to their territory, he or she is exposed to malicious communication or comment and invasions of privacy. Users who publicise personal contact details on Internet sites are especially vulnerable to harassment which can be very distressing and very difficult to control.

27. We asked Jim Gamble, Chief Executive Officer of the Child Exploitation and Online Protection Centre (CEOP), how dangerous the Internet was for children: he responded simply that "the Internet represents huge opportunity and risk".[39] The particular risks posed by new Internet-based services (such as video-sharing sites, social networking sites and virtual worlds) are chiefly those of exposure to harmful and inappropriate content, contact from people whose intentions are malicious, and incitement to dangerous or anti-social conduct. Some have found it convenient to list them as risks derived from content, contact and conduct.[40]

28. Those at risk are principally children, who are less well equipped to take decisions for themselves and to manage threats. Dr Byron observed that neural networks at the front of the brain are very underdeveloped at birth and that it is generally not until adolescence that the brain is sufficiently developed to evaluate and manage risk, differentiate between fantasy and reality, and regulate emotions.[41] Children may also be the target of exploitation for sexual purposes.

29. There is also a potential threat to adults who are depressed, or who have a tendency to self-harm, or who are emotionally unstable, who may find certain content disturbing; it may also be that content can have an adverse effect on sexual offenders or people with a tendency towards anti-social or criminal behaviour.[42]

[39] Q 194

[40] See *Byron Review*

[41] Q 340

[42] See Ev 18

Content-based risks

30. Content-based risks have long been recognised in broadcasting and in film, and it is generally accepted that children will find certain material unacceptably shocking and disturbing, even if less currency perhaps is given nowadays to the notion that content might "deprave and corrupt", to use the term from the Obscene Publications Act 1959.[43] The same risks are present in content on the Internet, which will encompass not just broadcast programming but also on-demand entertainment, user-generated content and material made available through pressure groups and interest groups. The distinctive feature of the Internet, however, is the ease of access and the ready availability of potentially harmful material: the Children's Charities' Coalition for Internet Safety (CHIS) warned of the Internet's capacity to provide information "in an uncontrolled way which can be damaging to children".[44]

31. CHIS told us that "children are known to come across and download age-inappropriate content or disturbing and upsetting material".[45] A joint submission from Professor Sonia Livingstone and Andrea Millwood Hargrave cited research suggesting that 16% of 8–15 year olds in the UK have come across "nasty, worrying or frightening" content online; they observed that this finding was repeated in other countries, sometimes with higher estimates.[46]

32. The main concern for many parents is that children will come across pornography while searching the Internet. CHIS noted the "sheer volume" of pornographic material that is in circulation and the ease of access to it.[47] Such content is likely to be hosted outside the UK: the Internet Watch Foundation told us that it had not identified within the last two years any content hosted on UK servers which might fail the test of obscenity under the Obscene Publications Act 1959.[48]

33. Other types of content, although perhaps less widespread, may in fact be no less threatening. The Government pointed out that terrorists used the Internet as an operational platform and as a tool for radicalisation and recruitment.[49] Some websites set up by fringe groups encourage illegal acts (such as assisted suicide) or incite hatred; others feature extreme, sadistic or graphic violence. Childnet International pointed out that not all information accessible on the Internet was necessarily accurate; both children and adults could be at risk, for instance, from misleading health advice.[50] Internet chatrooms can attract comments which are abusive or explicit and which others find distressing.

---

[43] The provisions of the Obscene Publications Act 1959 were applied to television and sound broadcasting by section 162 of the Broadcasting Act 1990, which specified that inclusion of any matter in a programme was "publication" within the meaning of the 1959 Act. Prosecutions for obscenity in audio-visual material are a matter for the police rather than for Ofcom: Annex 3 to Ofcom memorandum [*not printed*]

[44] Ev 4

[45] Ev 4

[46] Ev 16

[47] Ev 4

[48] If the effect of the material is, if taken as a whole, "such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it". See also Ev 43

[49] Ev 346

[50] Ev 10

34. Occasionally potentially illegal or harmful content, such as material which features violence or is sexually explicit or which is inflammatory or incites hatred, is uploaded to interactive sites featuring user-generated content. The Internet Watch Foundation, a self-regulatory body seeking to minimise the availability of potentially illegal or otherwise harmful content on the Internet,[51] told us that it had received just over 150 reports about material on social networking sites since 2005; on examination, none of the material was thought to be potentially illegal. At one point, there had been a growth in the number of reports about potentially illegal child sexual abuse content hosted on photo-sharing websites, although the Internet Watch Foundation noted that larger companies had since improved their security and abuse management policies.[52] We note the observation by Ofcom that public concern about harmful content appears to be more acute for sites which host user-generated content and which offer a "general use proposition" rather than those which are niche sites with a stated objective to share pornography or violent content.[53]

35. There has also been concern about the use of virtual worlds (such as *Second Life*) where, although no-one in particular is a target, users have created avatars which have then simulated sexual abuse of children.[54]

36. Certain video games have become notorious for their violent content. Manhunt, released in November 2003, is set in a lawless imaginary city populated by violent gangs of white supremacists, psychotic psychiatric patients and black magicians. The main character, whom the player 'directs' through the game, is a criminal on death row who proceeds to take on opponents and kill them. The distinctive feature of Manhunt is the brutality and the sadistic detail of the combat. A sequel, Manhunt 2, was released in March 2008. Initially, the British Board of Film Classification (BBFC) refused to award any classification because of its "unremitting bleakness and callousness of tone" and its "unrelenting focus on stalking and brutal slaying". The BBFC's decision was challenged and ultimately overturned in the High Court. Although the game has now received an 18 classification, the game's publisher, Rockstar Games, has still not released the game onto the UK market.

37. Other controversial games include those from the Grand Theft Auto series, set in the underworlds of fictional cities. Players take on the role of lowlife criminals who, by carrying out bank robberies, assassinations or other criminal acts, rise through the ranks of the fictional cities' organised crime networks. Unlike Manhunt, games in the Grand Theft Auto series do include non-violent sequences and also feature a good deal of humour and irony. The latest edition has been hailed as taking gaming to the next level but it is clearly designed for adults and should be restricted to them.

Contact-based risks

38. The Internet is an interactive public forum and one of its strengths is the ease of communication which it allows regardless of borders. This very ease of communication,

---

[51] See paragraph 71

[52] Ev 45-46

[53] Ev 254

[54] Such activity led to a police investigation in Germany in May 2007: see *Guardian* 8 May 2007

however, which enables strangers to converse with each other, enables contact which is not sought and which may not be well-intentioned. Posting personal details or images on social networking sites can lead to uninvited contact from others, whose identity may be shrouded. As Mr Angus, Executive Vice-President and General Counsel for Fox Interactive Media, said, "people are not always who they say they are" and children need to make sure they know who they are talking to.[55] In the worst cases, sexual predators may use a casual exchange as a starting-point for a more intense relationship and "grooming". The Children's Charities' Coalition on Internet Safety (CHIS) described the Internet's capacity for facilitating sexual abuse of children "by persuading and manipulating them into secretive relationships or meetings with abusers or potential abusers". It added that "such sexual abuse may be contact abuse (through a meeting in the real world) or non-contact (through webcams and other means).[56]

39. CHIS observed that chatrooms, social networking sites and other online fora were places where it was known that children might be identified and targeted.[57] Users of social networking sites provide personal details to build up "profiles" which can, if not carefully managed, be viewed by any other subscriber. Childnet International told us that children and young people were not discriminate about the information which they posted on social networking sites and that many young people uploaded music, images or videos without thought about long-term consequences.[58] Ofcom presented research suggesting that many users of social networking sites did not conceal their personal details and often included in their profiles their names, where they lived, the schools they attended or their places of work. Some also published their Instant Messenger account details. Some were unaware that the default privacy settings for their profile were "open", allowing people they did not know to see their page and their personal details. Many seemed unwilling to consider that there could be a risk attached to social networking.[59]

40. Professor Livingstone and Ms Millwood Hargrave cited a study by the Child Exploitation and Online Protection Centre (CEOP) suggesting that 25% of children and young people have gone on to meet someone in person that they first "met" online, although no data was available to quantify the harm, if any, caused.[60] Research conducted by Professor Livingstone and published in 2005 suggested that 46% of 9 to 19 year olds have divulged personal information to someone that they have met online.[61]

Conduct-based risks

41. Children may be bullied by other children through use of new communications technologies, a practice commonly termed "cyber-bullying". Typically, photographs or videos may be taken of a bullying incident; those images are then circulated using mobile phones or video-sharing websites, "scaling up" the event and the potential distress caused.

---

[55] Q 387

[56] Ev 3

[57] Ev 3

[58] Ev 11

[59] Ev 229

[60] Ev 17

[61] Ev 117

Different studies (based on different age groups) have yielded different figures for the proportion of children and young people who had been bullied by text, Internet or e-mail, but there is consistent evidence that between 10% and 20% of children have been cyber-bullied,[62] with girls more likely than boys to have suffered.[63] CHIS remarked upon the existence of "a great deal" of research evidence to show that bullying can have a devastating impact on children's social and emotional development".[64]

42. The ease of distribution of images using mobile phones and the Internet can also encourage exhibitionist conduct. A recent and unwelcome practice is that of "happy slapping"—essentially a filmed assault (often using a mobile phone camera) which is then shared either among friends or with a wider audience, by being uploaded onto a site which hosts user-generated content. A BBC Panorama programme broadcast in June 2007 reported videos of children as young as 11 or 12 kicking and punching other children in the head. In one case, onlookers shouted "kill her"; in another, a 15-year-old girl was knocked unconscious and suffered a detached retina. Other types of conduct which might be filmed and uploaded to such sites include dangerous driving, displays of what appear to be firearms, and dangerous stunts or "dares" (for instance on railway tracks). Such content may not be illegal and may not, in some cases, even breach the Terms of Use drawn up by the site owner.[65]

43. Some conduct—such as posting images of other people or comments about them on social networking services—may not be calculated to distress or shock but may nonetheless be deeply hurtful.

44. Witnesses suggested that video games could cause harm not just because of their content but also because they could be addictive. The Children' Charities' Coalition for Internet Safety (CHIS) reported that there was "a great deal of anxiety about excessive use of games" and possible consequences in deflecting children from schoolwork and the development of social skills.[66] David Cooke, Director of the British Board of Film Classification, cited evidence that people were playing games for more than 24 hours on end; he maintained that "with online gaming you are also incentivised to go on playing because you may lose your position […] if you do not go on playing very regularly."[67] Mr Carr, Executive Secretary of the Children's Charities Coalition for Internet Safety, said that in some countries there had been cases of children "dying at the console of exhaustion".[68] It is also alleged that video games may lead to low levels of physical activity and, potentially, to obesity.

---

[62] Ev 17. See also Mr Carrick-Davies, Q2 and Microsoft Ev 39. An early study by Goldsmith's College suggested a figure of 22%.

[63] Research by Goldsmiths' College and the National Children's Home: see Third Report from the House of Commons Education and Skills Committee, *Bullying,* Session 2006-07, HC 85, Ev 92

[64] Ev 4

[65] See Ofcom Ev 256

[66] Ev 2

[67] Q 570

[68] Q 3

How real is the risk from exposure to harmful content?

45. A great deal of effort has been expended in debating and trying to establish whether certain types of content cause direct harm and whether exposure to violent content could cause violent behaviour. The issue has surfaced in this House from time to time, frequently in relation to the murder of Stefan Pakeerah in Leicester in February 2004: it is alleged that the behaviour of his attacker was triggered by playing *Manhunt*, a video game in which players are able to simulate violent killings.

46. The debate about the effects of violent or sexual content is not a new one and has raged whenever the boundaries of what was deemed permissible content in visual entertainment have been stretched or following particularly harrowing events. Given the uncertainty about whether any causal link between viewed violence and subsequent behaviour exists, we asked Ofcom about the rationale for controls (such as the nine o'clock watershed) applied to content on television. Ofcom was satisfied that, on the balance of probability, there is a potential harm to children from exposure to certain content, and it noted that "very few people have actually challenged that".[69]

47. The definition of what is "harmful" is not hard and fast: for one ten-year old a scene will seem very real and disturbing, whereas another will be able apparently to dismiss it or treat it as fantasy (although this does not necessarily mean that some form of harm does not occur).[70] Both children and young people may find it hard to interpret or filter information. Equally, as Dr Byron pointed out, one parent might take the view that children should not see certain content, whereas another might judge that it was instructive and "empowering" for a child to be aware that such content existed.[71] That is a judgment for each parent to make.

48. Dr Byron identified the causal question as a key issue for her Review, as did Ofcom, which commissioned Professor Sonia Livingstone and Andrea Millwood Hargrave to update a review of research evidence published in 2006 on content-related harm across a variety of media.[72] The outcome remains uncertain, with the debate polarised between those who believe that there is evidence of a causal link and those who challenge the methodology underlying that evidence. One submission, from Professor Julian Petley,[73] described this debate as "an unbridgeable chasm between two entirely different kinds of research".[74] Dr Byron concluded that "there is some evidence of short term aggression from playing violent video games but no studies of whether this leads to long term effects" and also that "there is a correlation between playing violent games and aggressive behaviour, but this is not evidence that one causes the other". She points out that "arousal brought on by some games can generate stress-like symptoms in children" and that "games are more likely to affect perceptions and expectations of the real world amongst younger

[69] Q 504

[70] See Professor Livingstone Q 29 and 31

[71] Q 342

[72] Ev 189

[73] Professor of Film and Television at the School of Arts at Brunel University

[74] Ev 361

children, because of their less developed ability to distinguish between fact and fiction".[75] Ofcom said that, for adults, "it seems that playing violent video games is associated with emotional tension and arousal during play, and it may increase feelings of hostility to others or aggressive thoughts and behaviours following play", although it noted uncertainty about whether such effects would occur in real life (rather than just in experimental conditions) and whether such effects would last beyond the period immediately after game play.[76]

49. Representatives of the games industry challenged the assertions that violent games led to violent behaviour. The Entertainment and Leisure Software Publishers Association (ELSPA) told us that "no credible evidence exists clearly linking gameplay with psychological or sociological risk" and that "no credible evidence exists linking combative gameplay behaviour with violent or anti-social behaviour in real life".[77] Dr Richard Wilson, chief executive officer of Tiga, said that "when we look at violent behaviour in society I am sure the evidence will show there is a much stronger link, for example, between alcohol abuse and violent behaviour".[78]

50. The research base for assessing the possible harmful effects of sites which provide information about (and possibly encourage) suicide, or eating disorders, or those which project "hate speech", is less well documented. Ofcom noted that little or nothing was known about how young people (especially those from targeted groups, such as ethnic minorities) respond to hateful content.[79]

51. The conclusion overall is that there is still no clear evidence of a causal link between activity or behaviour portrayed on-screen and subsequent behaviour by the person who viewed it.[80] Professor Livingstone and Ms Millwood Hargrave told us that the research evidence was "too patchy", particularly in relation to new media platforms. Other witnesses bore out this conclusion: the Children's Charities' Coalition for Internet Safety (CHIS) told us that "we do not know how or whether the sheer volume of pornographic material in circulation on the Internet, or the ease of access to it, affects children in terms of a distortion of their 'normal sexual development'". CHIS said that there had been no major research studies into the subject and that it was difficult to track the impact of exposure.[81]

52. Dr Byron's conclusion on the addictive nature of video games was ambivalent. She said in her Review that "we need to consider whether excessive gaming by children is due to the addictive nature of video games for them or if it is more a matter of parents not feeling able to manage their children's behaviour effectively. […] Research has yet to determine whether some types of game are more addictive than others or whether there are inherent features, either individual characteristics (e.g. children with obsessive compulsive tendencies) or circumstantial features (e.g. children in situations of boredom) that predict

[75] *Byron Review*, p 11

[76] Ev 245

[77] Ev 163

[78] Q 455

[79] Ev 16; Ofcom Ev 244

[80] For instance DCMS/BERR memorandum Ev 346

[81] Ev 4

high usage".[82] Dr Byron noted the ethical difficulty of undertaking research through exposing children to potentially harmful material, as did Mr Carr.[83]

53. Professor Livingstone and Ms Millwood Hargrave argued that "to look for simple and direct causal effects of the media is not appropriate". They concluded, from their review of research literature on behalf of Ofcom, that there was "a lack of evidence for actual harm but evidence for the risk of harm".[84] However, the absence of any evidence of harm to children from the Internet does not necessarily prove that children are not being harmed;[85] and the lack of evidence of harm directly caused by exposure to content does not mean that there should not be controls. Dr Byron recommended that the protection of children from online dangers should be based on *probability* of risk.[86] Her conclusion echoes that of Professor Livingstone and Ms Millwood Hargrave, who proposed "a risk-based approach, which argues for the likelihood of risk rather than inevitable harm".[87] **We agree that any approach to the protection of children from online dangers should be based on the probability of risk. We believe that incontrovertible evidence of harm is not necessarily required in order to justify a restriction of access to certain types of content in any medium.**

54. However, risks are part of growing up. Childnet International noted that it was important for children and young people to learn to understand, assess and manage risks, both online and offline, as part of the process of growing up.[88] Dr Byron, both in her evidence to us and in her Review, warned of a risk-averse culture and a "zero-risk" approach to parenting which, by restricting children's opportunities to take risks, socialise and develop, was causing children to take risks in an online environment which was poorly understood by adults.[89] We agree. **It is sensible that parents set boundaries for their children's online activities, but a totally risk-averse culture in parenting will not equip children to face dangers which they will inevitably encounter as they grow older.**

4 Controlling risk

55. Dr Byron, in her Review, noted that risks were a reality of life in the online world.[90] Certainly, we cannot see any immediate prospect that existing causes of risk will diminish or disappear of their own accord. Therefore, the aim of public and private company policy, as Bebo observed, should be to minimise risk and to provide consumers with the knowledge and tools they need to address potential harm if and when they encounter it.[91]

[82] *Byron Review,* p 153

[83] Q 3; Q 342

[84] Ofcom, Ev 248

[85] Q 20

[86] Q 341

[87] Ev 18

[88] Ev 9

[89] Q 339

[90] See for instance *Byron Review* Executive Summary, paragraph 12

[91] Ev 144

Traditional media

56. Measures to control risks from access to potentially harmful content broadcast on traditional media are well established. The Broadcasting Code administered by Ofcom guides broadcasters on the concept of harm and offence and on how it should be respected in programming policy. Broadcasters observe the nine o'clock watershed, a point after which it may be assumed that younger children will not be watching television or, if they are watching, will be doing so with the permission of their parents. However, the concept of the "watershed" is now being eroded by the 24-hour availability of material on demand or from archives, as well as the increasing number of personal video recorders. The EU Audio Visual Media Services Directive promulgated in 2007 requires each Member State to draw up a new regulatory framework for on-demand video services. Ofcom told us that the UK was in the early stages of developing the model, which was likely to be one of co-regulation, defined as self–regulation backed by statutory powers.[92] Regulation of on-demand services is currently exercised by a self-regulatory body, the Association for Television on Demand (ATVOD), whose members are required to adhere to the Association's code of practice. The ATVOD Board updates the code with practice statements which are binding on ATVOD members.[93] Ofcom told us that "effective and consistently applied content information is likely to be a significant element" of a future regulatory framework for on-demand services, along with measures such as PIN numbers to control children's access to potentially harmful content.[94]

57. Films have likewise been classified and accorded ratings, some of which specify a minimum age at which it is deemed that any risks from content can be managed. Films for cinematic release or for DVD are classified by the British Board of Film Classification (BBFC); the admission of children to a film or the sale of a video recording or DVD must be restricted in accordance with that classification. Breach of the conditions of a classification is an offence under criminal law. The British Board of Film Classification also has responsibility for classifying certain video games; we consider the BBFC's future role in games classification in Section 6.

Existing structures for protection from harmful content on the Internet

The Home Office Taskforce

58. Certain bodies have been established by the Government to help manage the risks arising specifically from the Internet. The most all-embracing is the Home Office Taskforce on Child Protection on the Internet, formed in 2001 to bring together the Government, online technology providers, statutory and non-statutory bodies, law enforcement and child protection specialists. Main meetings are chaired by the Home Secretary or by the Minister responsible for child protection. The Home Office provides the secretariat, and a Programme Board comprising representatives from industry, charities, the Child Exploitation and Online Protection Centre (CEOP) and Government departments sets the

[92] Q 525

[93] Annex 3 to Ofcom memorandum [*not printed*]

[94] Ev 253

direction. So far, the Taskforce has issued various sets of good practice guidance, recommendations for changes to the criminal law, and the development of training for professionals involved in child protection.

59. The Home Office Taskforce was much praised in evidence and is widely regarded as a good example of collaboration between the Government and the Internet-based industry. Mr Galvin, representing BT,[95] said that the Task Force "has proved to be a vital piece of glue to bring together the industry";[96] and Dr O'Connell, Chief Safety Officer at Bebo and a member of the Task Force, said that it was viewed "round the world as a model of good practice".[97] The Children's Charities' Coalition for Internet Safety (CHIS) said that the Task Force had "become a major element within the UK's self-regulatory regime and that it "undoubtedly has performed and continues to perform an extremely valuable function".[98] It spoke of "the enormous importance which we and the industry attach both to being able to work together in this way and to being able to engage directly with senior Ministers in the Government". CHIS said that "anything which removes or weakens that political link will also weaken the political impact of the policy".[99]

60. Dr Byron's report recommended that the existing Task Force should be transformed into a new UK Council for Child Internet Safety, with a strengthened secretariat and responsibility for leading a strategy across Government. She envisaged that the Home Office and the Department for Children, Schools and Families would chair the Council, with the roles of other Government departments, especially the Department for Culture, Media and Sport, "properly reflected" in working arrangements. Dr Byron also recommended that the Council should appoint an advisory group with expertise in technology and child development, should listen to children, young people and parents, and should have a rolling research programme.

61. We asked Dr Byron how the new Council would differ from the Task Force. She commended the Task Force, which she said was "a model of good practice" and demonstrated that the UK has taken a responsible lead in thinking about the protection of children from potential dangers of the Internet. However, she saw a need for a body which was "properly resourced" with "more of a cross-Government feel", noting that the Internet industry was "very fatigued" at the different Government departments having "several sometimes contradictory conversations" with the industry.[100] The Children's Charities' Coalition for Internet Safety was particularly critical of the level of resources and staff support which had been devoted by the Government to the Task Force, which had never had its own budget or any staff solely dedicated to its work. The Coalition told us that the Task Force had had to rely upon underspends from other programmes for funding, and key officials had occasionally been redeployed without consultation.[101] Bebo also remarked upon the need for a co-ordinating body such as the Task Force to have dedicated civil

[95] Managing Director, Global Customer Experience Programme

[96] Q 252

[97] Q 432

[98] Ev 1

[99] Ev 1

[100] Q 347

[101] Ev 1

servants, a budget and proper standing.[102] Bebo's Chief Safety Officer, Dr O'Connell, suggested that the establishment of a UK Council would facilitate communication between the industry and the wider public, the media, Members of Parliament and others.[103] The Government argued that it was time for the Task Force "to move on to the next level" and to become a body "which will have additional traction in order to make progress". Mr Coaker, Parliamentary Under-Secretary of State at the Home Office, added that the new body would be more "all-embracing" and would look at access not just to illegal content but also to content which was legal but harmful and inappropriate.[104]

62. **The Home Office Task Force on Child Internet Safety has, by common consent, done good work and has served its purpose well; but its loose funding and support structures have given the impression that its work is of a comparatively low priority. We agree with Dr Byron that the structure and funding of the Task Force should be formalised. We also welcome the announcement by the Government that the date for establishment of the Council is to be brought forward from April 2009 to September 2008. However, we are concerned at reports from some key players that there has been no contact with Government to take this forward and from others that there has been little opportunity to influence decisions as to how the Council will operate in practice. We expect the Government to address these issues urgently.**

63. Ofcom is a member of the Home Secretary's Task Force and has been invited to join the Council.[105] We explored what sort of role Ofcom might have in the Council's work. Ofcom itself suggested to us that it might have a research role or that it might assist in co-ordinating codes of practice.[106] Mr Coaker saw a role for Ofcom in monitoring whether the work of the Council was actually being reflected in changed practice and better procedures in the industry.[107] Ed Richards, Chief Executive Officer at Ofcom, proposed that the Council and industry should concentrate on trying to achieve early effectiveness of self-regulation, perhaps with a role for Ofcom in assessing progress made.[108] Dr Byron did not envisage that the Council itself would have powers of sanction against the industries involved. Ministers suggested that the reputation of individual companies whose practices lagged behind would be damaged and that they would appear less attractive to advertisers as a result; therefore there was a financial incentive to demonstrate good practice.[109]

64. We asked the Government to explain why the Council was to be co-chaired by the Home Office and the Department for Children, Schools and Families. It replied that the Council would evolve from the Home Secretary's Taskforce and that it was therefore appropriate for the Home Office to co-chair the Council; and it argued that the importance of the Council's work in educating parents and young people on Internet safety justified a co-chairing role for the Department for Children, Schools and Families. Other

[102] Q 440

[103] Q 441

[104] Q 580

[105] Q 588

[106] Q 511

[107] Q 589

[108] Q 534

[109] Mr Brennan Q 591

Departments, including the Department for Culture, Media and Sport, would merely have "a crucial role".[110]

65. We asked Dr Byron what budget should be allocated to the Council. She said that she had "not thought about money" and "would not know"; but she urged that enough money be allocated to target effectively and creatively.[111] The Government appeared confident that it had a good idea of the likely resources needed, although it did not give an explicit guarantee that it would fund the Council's expenditure in full.[112]

66. **We agree that the Council, at least in its early years, should be chaired by a Minister, to ensure that Council members have direct access to public policy-making. However, we question the proposed joint chairing arrangement, which excludes DCMS Ministers. We believe that it would be unfortunate if DCMS were to appear subsidiary in Council governance, given its role in media regulation, although we recognise the practical difficulties in sharing the chairing role between many Departments: indeed, we question whether co-chairing is desirable in principle. We invite the Government to consider carefully whether to appoint a single lead minister, either from one of the Departments represented or perhaps from the Cabinet Office. There may be a case in future for the Council to be chaired by someone who sits outside Government, particularly if the role of the Council is to expand. Given that the Government has accepted Dr Byron's recommendations in full, we believe it should now move quickly to provide a budget.**

67. The work of the UK Council on Child Internet Safety as proposed by Dr Byron has not yet been fully defined: terms of reference and a work plan will be agreed by the Executive Board in September 2008.[113] We expect that there will be a significant early effort in certain areas, such as drawing up guidance and setting minimum standards, for instance on the time taken to remove potentially harmful content. **While there might be an expectation that most of the Council's effort would be directed towards child protection, we believe that there is a danger of overlooking possible harm to vulnerable adults, and we recommend that the Government should give this proper consideration when deciding the Council's terms of reference.**

The Child Exploitation and Online Protection Centre

68. More recently, in recognition of the distinct threat of sexual exploitation through the Internet, the Government established the Child Exploitation and Online Protection Centre (CEOP), essentially a national law enforcement and child protection agency affiliated to the Serious Organised Crime Agency but retaining full operational independence.[114] CEOP told us that its purpose was:

- "to identify, locate and protect children from sexual exploitation and online abuse;

[110] Mrs Hodge Q 579

[111] Q 379 and 380

[112] Q 597-598

[113] Byron Review Action Plan page 6

[114] Ev 87

- to engage and empower children, young people, parents and the community through information and education; and

- to enhance existing responses by working with industry to make the online environment safer by design and by improving the management of high risk offenders".[115]

CEOP deals primarily with cases referred to it and receives on average between 450 and 550 reports per month.[116] Dr Byron commended CEOP strongly for its work;[117] so did Mr Coaker, Parliamentary Under-Secretary of State at the Home Office, who described the Centre's Chief Executive Officer, Mr Gamble, as "excellent" and "a trailblazer".[118]

69. When we took evidence from Mr Gamble in March 2008, he pressed for more funding for CEOP, partly to meet the extra demand arising from abuse of social networking services and to deal with a backlog of cases. He estimated that there was a backlog of about 700 cases, albeit ones in which there was least evidence of a need for urgent action.[119] He also spoke of "huge pressure on our referral staff" and noted that "you cannot switch off the tap".[120] The Home Office told us that it had provided £5.65 million for CEOP in 2007–08: this had been supplemented by £3.19 million in cash and in kind from various sources, including Government departments, charities and industry. For 2008–09, the Home Office has provided a budget of £5.77 million; figures for contributions from other Government departments, charities and industry are not yet available.[121] The Home Office said that while it had not received a formal request from CEOP for more funding, it would of course consider any approach made; and it stressed that it was inconceivable that the Government would not fund CEOP in the future.[122]

70. **We are much impressed by the work of the Child Exploitation and Online Protection Centre and its close co-operation with charities such as the National Society for the Prevention of Cruelty to Children. However, we are concerned that levels of funding are not keeping pace with the increasing volume of work which is referred to the Centre, and we therefore encourage the Government to look favourably on any request by CEOP for increased resources. We also welcome the financial contribution made by charities and industry, and we believe that the latter should be increased: business models for Internet-based services rely upon public confidence that networking sites are safe to use, and CEOP plays a large part in delivering that safety.**

[115] Ev 87

[116] Q 168

[117] Dr Byron Q 337 and Q 354

[118] Q 595

[119] Q 177 and 178

[120] Q 179 and Q 180

[121] Ev 402

[122] Q 615 and 620

The Internet Watch Foundation

71. Businesses which provide Internet content, access and services, either from fixed terminals (such as PCs) or from mobile devices, have recognised the particular dangers posed by certain types of content on the Internet. In 1996, the Internet Watch Foundation was formed as a self-regulatory industry body, to minimise the availability of potentially illegal or otherwise harmful content on the Internet, and to take action to prevent exposure to illegal content, in particular by:

- operating a hotline enabling the public to report such instances;
- operating a notice and takedown service to alert hosting service providers of criminal content found on their servers; and
- alerting relevant law enforcement agencies to the content.

All major Internet service providers and search engines are members of the Foundation, as are all mobile network operators.[123]

72. The Foundation's Board aims to minimise the availability of potentially illegal Internet content, specifically:

- child sexual abuse images hosted anywhere in the world;
- criminally obscene content hosted in the UK;
- content inciting racial hatred hosted in the UK.[124]

For illegal content hosted in the UK, the Foundation may issue a "take-down" notice to the content host. If the content host fails to comply, it becomes liable to prosecution.[125] Mr Galvin, representing BT, told us that he could not think of a single example when an Internet service provider had refused to take down a site once it had been requested to do so.[126] If the content is hosted outside the UK, the Foundation has no powers to require the site host to take down the material: it told us that "we do not have any relationships with any other government or any other hotline in the world to put them on notice about these types of websites".[127] It will, however, inform the relevant authorities and add the website to its database of addresses hosting illegal content.[128]

73. The overwhelming majority of domestic consumers' Internet connections are operated by Internet service providers (ISPs) which block access to sites listed in this database. All major search engines block access to such sites.[129] The Foundation claimed that it had

[123] Ev 76, Ev 42

[124] Ev 42

[125] DCMS memorandum Ev 347

[126] Q 208

[127] Q 59

[128] Ofcom, Ev 262

[129] See Ev 44. Microsoft told us that the list of URLs on the Foundation's list had been applied to its Live Search filters so that none of them would ever appear within search results using Live Search:Ev 35

achieved "remarkable internationally recognised success" in that, since 2003, less than 1% of reports of online child sexual abuse content processed by the Foundation had been traced to content hosted in the UK, compared to 18% in 1997.[130] However the Chief Executive of the Internet Watch Foundation did tell us that, with a degree of technical knowledge, it is possible to circumvent the blocks imposed.[131]

Other self-regulatory structures and codes

74. Some businesses providing services using the Internet or other new media have themselves taken steps to draw up minimum standards. In some cases, these standards have been agreed with other interested parties, through the Home Office Taskforce on Child Protection on the Internet. In December 2005, for instance, the Taskforce published good practice guidance for providers of search services, stressing the importance of early advice to users on the risks and recommending that search providers should offer filters and clear facilities for users to report inappropriate material. Most recently, the Taskforce has published good practice guidance for providers of social networking and other user-interactive services: this guidance includes safety tips for parents and for children and young people.[132]

75. Mobile network operators adhere to a Code of Practice on New Forms of Content, drawn up in 2004. The Code covers classification of commercially supplied content, access controls for content classified as being unsuitable for people under 18, provision of parental controls to restrict access to internet sites, action against bulk communications and malicious communications, and the provision of information and advice on protection. O_2 said that the Code had been widely recognised as a model of best practice, had been adopted by mobile operators in a number of other countries, and formed the basis of the EU Framework for Safer Mobile Use. Under this framework, mobile phone operators in EU Member States have committed to control access to adult internet content, run awareness-raising campaigns for parents and children, and classify commercial content according to national standards of decency and appropriateness.[133] We note that the effectiveness of the Code is being reviewed by Ofcom and that network operators will be undertaking a separate consultation exercise on updating the Code.[134]

76. Content provided by third parties (such as film clips or video games) and accessible using mobile devices is classified by the Independent Mobile Classification Body, using a framework based on existing standards in other media.[135] The only distinction made is between "18–rated" and "unclassified";[136] it is difficult to verify other age distinctions remotely.[137] T-Mobile told us that in three years there had been no official complaints

[130] Ev 42

[131] Q 53-4

[132] Home Office, April 2008

[133] Ev 66; see also www.europa.eu.int

[134] O_2 memorandum Ev 68

[135] Ev 61

[136] Ev 61

[137] Q 109

upheld by the IMCB and that the classification framework was well understood by those providing content for viewing on mobile devices; and it added that obligations to meet the requirements of the Code were contained in all service contracts.[138] Mr Carrick-Davies, Chief Executive of Childnet International, said that the mobile industry had "done a great deal of work in this country in identifying a code of practice which gives parents greater choices", largely through filter settings for Internet access. The difficulty, he believed, lay in ensuring that parents were aware of the options.[139]

Controlling content-based risks

77. The contrast between the care taken to regulate content broadcast using traditional means—through dedicated regulators, codes and sanctions—and the near absence of control over access to Internet content is striking. However, it is incorrect to assume that the Internet is beyond all regulation. Mr Purvis, Partner for Content and Standards at Ofcom, pointed out that "it is not as if there is a completely wild west on the Internet: the Internet content creators are subject to the law of the land like any other content creators".[140] Likewise, Mr Carrick-Davies, Chief Executive of Childnet International, stressed that the Internet was "not some moral vacuum" and that there were "some very good existing laws" applicable to providers of both online and offline services.[141]

78. There are several main approaches to the control of access to illegal or potentially harmful content. These include:

- Making it illegal to possess or distribute material, thereby prompting Internet service providers that become aware of such material to block access to it or take it down if they host it;
- For material which is undesirable but not illegal, website owners or hosts may take down content which is unacceptable under their Terms and Conditions or Acceptable Use policies;
- Filters can be applied at network level;
- Consumers may exercise discretion by applying filters locally.

Designation of content as illegal

79. It is already an offence to publish or distribute certain types of content on the Internet or anywhere else: these include indecent images of children, material which is deemed obscene and likely to "deprave or corrupt", words intended to stir up racial hatred, and statements likely to be understood as encouraging terrorism. The Internet Watch Foundation told us that a recent interpretation of the Obscene Publications Act 1959 had

[138] Ev 62

[139] Q 32

[140] Q 505

[141] Q 19

determined that the presence of explicit pornography on the front page of a website hosted in the UK, which a child under 18 might see, may fail the test under the Act.[142]

80. In certain cases it is not merely publication which is illegal: it is an offence to *possess* indecent images of children,[143] extreme pornography[144] (but not other pornography, even though it may fail the "publication" test under the Obscene Publications Act 1959), and any "terrorist publication" if it can be demonstrated that it is possessed with a view to distribution or provision to others, including by electronic means.[145] Downloading such material from the Internet, including images, is likely to constitute "possession". The Internet Watch Foundation told us that 12% of the reports of alleged criminal obscenity which it received would fail the new offence of possession of extreme pornography.[146] The Mobile Broadband Group confirmed that mobile network operators would respond to "notice and take down" requests from the Foundation which related to extreme pornography hosted in the UK.[147]

81. Conceivably, a person may come across by chance material on the Internet which it is illegal to possess. The Government told us that the new offence of possession of extreme pornography was not intended to target those who accidentally come into contact with obscene pornography.[148] We note that the Internet Watch Foundation told us that the decision by Internet service providers, mobile operators and search providers to block access to or take down sites displaying harmful or illegal material had been motivated by a desire to protect consumers from "stumbling across" potentially harmful or illegal content by accident.[149]

82. The Internet Watch Foundation will also prompt Internet service providers to bar access to sites which publish content which would be unlawful if hosted in the UK. In 2007, the Internet Watch Foundation processed 847 cases of content reported as potentially inciting racial hatred and assessed 203 of those as being likely to do so; but only one report identified content which could be traced to a UK host and which could therefore be forwarded to relevant authorities in the UK.[150] It told us that it received reports of sites featuring mutilation or extreme and graphic violence, but such sites were rarely if ever hosted in the UK even though the material was available to consumers in the UK.[151]

83. The Government told us that it was dedicating resources to identify illegal material on the Internet, such as material which either incited or encouraged terrorism or would prove useful in the preparation and commission of terrorist acts. The Government said that "we

---

[142] Q 59

[143] Section 160 of the Criminal Justice Act 1988

[144] Section 63 of the Criminal Justice and Immigration Act 2008, expected to be in force from January 2009: HL Deb 25 June 2008 col. 250 (WA);

[145] Section 2 of the Terrorism Act 2006

[146] Ev 43

[147] Ev 76

[148] Ev 346

[149] Q 53

[150] Ev 43

[151] Ev 44

now want to work with ISPs and others in the industry to take a more proactive role in identifying this material so that it can be removed if hosted in the UK". For material which is hosted outside the UK, the Government said that it would "work with the industry to identify ways to limit the availability of illegal terrorism-related material".[152]

Removal of content for non-compliance with terms of use policies

84. Sites hosting content—particularly user–generated content—generally operate according to Terms of Use or their equivalent[153] which specify types of content (images or text) which, although not necessarily illegal, are deemed to be unacceptable.[154] Once such sites become aware that they are hosting material which crosses their threshold for content standards, they will normally take it down. For instance, Mr Galvin, representing BT, told us that a pro-suicide site would cross that threshold "by miles".[155] Microsoft told us that it would take down content which, for example, advocated terrorism, as being in breach of its terms and conditions.[156] The Internet Service Providers Association told us that Acceptable Use Policies helped to combat the illegal and inappropriate use of the Internet and encouraged consumers to behave responsibly online.[157] Mobile network operators similarly told us that they would exercise the right to refuse to host material or to remove a user's right to participate in a chatroom which they hosted if they were "unhappy" with behaviour or content.[158]

85. YouTube, for example, has developed Community Guidelines and Terms of Use, indicating what types of content are acceptable. The language used is clear, concise and accessible, as the following excerpts show:

- "There is zero tolerance for predatory behaviour, stalking, threats, harassment, invading privacy, or the revealing of other members' personal information. Anyone caught doing these things may be permanently banned from YouTube.

- We encourage free speech and defend everyone's right to express unpopular points of view. But we do not permit hate speech (speech which attacks or demeans a group based on race or ethnic origin, religion, disability, gender, age, veteran status and sexual orientation/gender identity).

- Graphic or gratuitous violence is not allowed. If your video shows someone getting hurt, attacked or humiliated, don't post it.

- YouTube is not for pornography or sexually explicit content. If this describes your video, even if it's a video of yourself, don't post it on YouTube. Also, be advised that we work closely with law enforcement and we report child exploitation".

---

[152] Ev 346

[153] Such as Community Guidelines, or Acceptable Use Policies, or taste and decency criteria

[154] See Q 223

[155] Q 228

[156] Q 65

[157] Ev 100

[158] Q 107

We note that, although someone intending to upload a video on YouTube would be prompted to read the Community Guidelines and Terms of Use, they can proceed to upload it without having done so and without even having ticked a box to say that they had done so.[159] **We strongly recommend that terms and conditions which guide consumers on the types of content which are acceptable on a site should be prominent. It should be made more difficult for users to avoid seeing and reading the conditions of use: as a consequence, it would become more difficult for users to claim ignorance of terms and conditions if they upload inappropriate content. The UK Council for Child Internet Safety should examine this at an early stage and produce recommendations as to how it is best achieved.**

86. **We are also concerned that user-generated video content on sites such as YouTube does not carry any age classification, nor is there a watershed before which it cannot be viewed. We welcome efforts by YouTube to identify material only suitable for adults, such as that containing foul language, and to develop potential controls to prevent children from accessing it.**

"Flagging" content

87. It is common for services which host or enable access to user–generated content to enable consumers to report or "flag" material which seems not to conform to the site's standards. Once content has been flagged, a member of staff will review the video to assess whether it violates the terms of use. Google (which owns YouTube) told us that the large majority of material which users flagged was reviewed (and if necessary removed) within one hour; more time was required in cases when it was not immediately clear whether a video was a documentary or whether it was promoting or glorifying violence.[160] It added that only a small fraction of user-generated content was flagged as harmful or inappropriate and that an even smaller fraction required removal, in which case the user would be notified. Repeated violations of YouTube's Terms of Use by a user will lead to deletion of their account.[161] Google supplied further information on "flagging" in confidence.

88. We raised with Google (which owns YouTube) a notorious case in which a video of alleged gang rape uploaded to YouTube was viewed 600 times before being removed from the site. Mr Walker, General Counsel for Google, suggested that those 600 views may in fact have included repeat viewings by a smaller number of people; but he accepted that a mistake had been made in that the video had been flagged for review but had not, through human error, been taken down from the site. Mr Walker told us that review procedures had been changed to reduce the likelihood of such an error occurring again.[162] He also said that the error represented "an infinitesimal percentage of the material which we are reviewing".[163] Google pointed out in a confidential supplementary memorandum that the

[159] Q 276 to 278

[160] Q 296

[161] Ev 117

[162] Q 316 to 321

[163] Q 317

exact details of the case were still under police investigation. Nonetheless, the system failed, and it is difficult to know whether or not this was an isolated incident.

89. Ofcom noted that it is not possible to determine empirically how effective site review processes actually are. It described YouTube's review process as being "opaque to the public" and added that "because it is impossible to determine what proportion of content is potentially harmful, there is no means to assess the overall effectiveness of the system".[164] Ofcom proposes that the industry might draw up a code under which those who make user-generated content available would increase the transparency of their review processes, for example by reporting on times for dealing with "flags" or reports and on communications with complainants. Ofcom suggested that, ideally, a code would include independent verification of performance.[165] We agree, and we return to this issue in paragraphs 99 and 153 below.

Preview and review of user-generated content

90. It is not standard practice for staff employed by social networking sites or video-sharing sites to preview content before it can be viewed by consumers. It was put to us that to pre-screen all material before it was published on the Internet would be impractical, because of the sheer volume of material being uploaded.[166] In the case of YouTube, this is approximately 10 hours of video every minute.[167] Instead, YouTube relies upon "millions of active users who are vocal when it comes to alerting us to content they find unacceptable or believe may breach our policies".[168] Google (which owns YouTube) also told us that "we don't, and can't, review content before it goes live, anymore than a telephone company would screen the content of calls or an ISP would edit e-mails".[169] We are not convinced that this is a valid analogy: a person who makes a telephone call or who sends an e-mail does so in the expectation that the content will normally remain private. Content uploaded to many websites is generally intended for public notice and may be accessible by a person of any age in almost any part of the world.

91. The BBC's guidelines for online services identify services which merit previewing of content, particularly sites which are designed to appeal to children or which invite users to send pictures by e-mail, or sites featuring live chat where users talk to a celebrity guest.[170]

92. Some companies are working on filters to screen material before it is uploaded to their sites. Mr Walker, General Counsel for Google, told us that technology existed to block automatically the reposting of videos that had already been deemed to violate Terms of Use and had been taken down.[171] He added that work was under way to develop software which

[164] Ev 254

[165] Ev 255

[166] Mobile Broadband Group Q 123

[167] Q 313

[168] Ev 119

[169] Ev 119

[170] Ofcom, Ev 273

[171] Q 279

could identify pornographic images and prevent them from being uploaded to YouTube.[172] The difficulty will be to refine the technology to the point where, for example, it can distinguish pornography from other images where flesh is exposed. Google observed in its written memorandum that "technology can sometimes help but it is rarely a complete answer".[173] Dr Byron indicated that research was under way to explore ways of scanning both an image and accompanying text to assess material.[174] Kevin Brennan, a Minister at the Department for Children, Schools and Families, clearly saw this as a possible way forward.[175]

93. Some companies actively review content once it has been uploaded. MySpace told us that it reviewed "each image and video that is uploaded to the MySpace server for compliance with the Terms of Use and Photo policy"; this was confirmed to us when we visited MySpace's offices in the US.[176] Several hundred people are employed by MySpace to review images and videos after they have been posted. Inappropriate material is normally taken down within two hours, although there is a target to reduce that to one hour.[177] Bebo also has a Member Media Review team which searches for inappropriate images and videos already uploaded to the site. Typically, such material is removed within 24 hours after it has been uploaded, although Bebo said that "it is impossible to find all inappropriate content".[178]

94. Some providers claim that the provisions of the E-Commerce Directive restrict their ability to take down material before there have been complaints about it. Under regulation 17 of the Electronic Commerce (EC Directive) Regulations 2002 (which transpose the Directive into UK law),[179] companies that transmit Internet content on behalf of others (such as a user's profile page on a social networking site) cannot be held liable for anything illegal about the content if they did not initiate the transmission, select the receiver, or select or modify the information contained in the transmission. Nor is a service which hosts Internet content liable for damages or for any criminal sanction as a result of that storage if they do not have "actual knowledge" of unlawful activity or information and if, on becoming aware of such activity, they act "expeditiously" to remove or to disable access to the information.[180]

95. Some ISPs and operators of social networking sites have expressed a fear that any effort which they make to scan content automatically could be interpreted by a court as meaning that they have "actual knowledge" of all the content they host, causing them to become liable in law for content which wrongly survives the scan. Dr Byron challenged this reasoning, arguing that such an approach "is a bit like saying that it is unfair to ask companies to survey their premises for asbestos in case they find some but fail to remove it

[172] Q 298. See also Q 305 and 306

[173] Ev 119

[174] Q 375

[175] Q 608

[176] Ev 150

[177] Information supplied to the Committee by MySpace in the US.

[178] Ev 147

[179] SI 2002 no. 2013

[180] See Ofcom, Ev 249

safely", and she believes that "on this issue, companies should not hide behind the law".[181] **We do not believe that it is in the public interest for Internet service providers or networking sites to neglect screening content because of a fear that they will become liable under the terms of the EC E-Commerce Directive for material which is illegal but which is not identified. It would be perverse if the law were to make such sites more vulnerable for trying to offer protection to consumers. We recommend that Ofcom or the Government should set out their interpretation of when the E-Commerce Directive will place upon Internet service providers liability for content which they host or to which they enable access. Ultimately, the Government should be prepared to seek amendment to the Directive if it is preventing ISPs and websites from exercising more rigorous controls over content.**

96. **We found the arguments put forward by Google/You Tube against their staff undertaking any kind of proactive screening to be unconvincing. To plead that the volume of traffic prevents screening of content is clearly not correct: indeed, major providers such as MySpace have not been deterred from reviewing material posted on their sites. Even if review of every bit of content is not practical, that is not an argument to undertake none at all. We recommend that proactive review of content should be standard practice for sites hosting user-generated content, and we look to the UK Council proposed by Dr Byron to give a high priority to reconciling the conflicting claims about the practicality and effectiveness of using staff and technological tools to screen and take down material.**

97. Mr Walker, General Counsel for YouTube, agreed to consider the possibility of using data on users' histories, numbers of people viewing an item, and video file labels to see whether there was an effective way to minimise the amount of controversial material posted onto YouTube.[182] **File titles and screening tools can help to identify files which appear to present a particular risk of exposure to inappropriate material. We encourage sites which handle user-generated content to develop as a priority technological tools to screen file titles and prevent the upload of—or quarantine—material which potentially violates terms and conditions of use until it has been reviewed by staff. We also encourage sites to share their knowledge and expertise at the UK Council on Child Internet Safety, with a view to developing codes of practice for prior screening of material.**

Take-down times

98. As already noted, almost all social-networking sites and those hosting user-generated content rely on their users to notify them of inappropriate material that has been posted. Once "flagged", it is then reviewed and if found to be in breach of the terms and conditions, it is taken down. We asked representatives of Internet service providers how long it took to take down content once notified. We were told that, for child abuse content, the industry standard was 24 hours, although that was "best practice" and the Internet Service Providers Association did not give us an assurance that it was consistently met.[183]

[181] *Byron Review* paragraphs 4.16 to 4.18

[182] Q 315

[183] Q 224 and 225

For content other than child abuse content, there might be a need for "greater reflection".[184] **We find it shocking that a take-down time of 24 hours for removal of child abuse content should be an industry standard.**

99. Dr Byron observed that companies may be unwilling to make specific public commitments to respond to breaches of acceptable use policies as quickly as possible (i.e. by taking down material) as they fear that such commitments might become part of a company's contract with users, exposing the company to litigation if it fails to meet the target (perhaps because of a surge in complaints).[185] She nonetheless recommended that sites should be encouraged to sign up to specific commitments on take-down times. The Chief Executive of Ofcom was particularly critical of the lack of clarity about take-down procedures.[186] **We believe that there is a need for agreed minimum standards across industry on take-down times in order to increase consumer confidence. We recommend that the UK Council on Child Internet Safety should work with Internet-based industries to develop a consistent and transparent policy on take-down procedures with clear maximum times within which inappropriate material will be removed. This should be subject to independent verification and publication.** We return to this issue in paragraph 153.

Filtering software

100. A large number of software suppliers specialise in providing software to protect customers and their children while on the Internet. All leading Internet service providers in the UK offer filtering products, and the majority of UK broadband subscriptions are offered with a free filtering package.[187] Such software enables parents to block access to websites considered to be unsuitable. Microsoft described its Family Safety Settings service, which allows parents to choose settings which allow, block or warn for a range of content categories, including Web-based chat and e-mail communications.[188] Google has developed its own SafeSearch filter, which will exclude webpages featuring pornographic or explicit content from search results.[189] The filter has three settings: no filter, filter pages with explicit images, and filter pages with explicit images or text.

101. Search filters can be effective, if crude. One of the inherent dangers is overblocking, which can become a safety issue. The BBC's submission to the Byron Review cited a report from one operator of online parental controls saying that "overblocking was the number one reason why parents turned off their parental controls". One filtering product was found to block access to the BBC's own site for children, CBBC. The BBC noted that a BSI kitemark standard was to be developed for online parental controls, and it urged that

[184] Q 224

[185] Byron Review paragraph 4.20

[186] Q 512

[187] Ofcom Ev 259

[188] Ev 35 and 36

[189] Ev 118

software should only receive the kitemark if it could demonstrate low levels of overblocking.[190]

102. Although most filtering tools under-block or over-block access to some extent, Ofcom cited evidence that such tools were indeed capable of filtering potentially harmful content without seriously degrading children's experience of the Internet.[191] The Internet Watch Foundation conducted a web search using unambiguous and explicitly adult terms with search filters switched off; search results returned over 10 million pages, with all of the links on the first three pages of search results linking directly to content which might be considered as potentially illegal under UK law if hosted in the UK and which would almost certainly be deemed inappropriate for children to view. The same search query with filters applied returned a list of 1.6 million web pages, most of which were online discussions or news items; no direct links to sexually explicit items were found. A similar experiment, this time including the word "teen" as a search term, generated a similar outcome.[192]

103. BT stressed the flexibility of "device-based controls", which could be applied in the home and which could permit different access regimes for use by different family members.[193] They nonetheless require an effort by parents or carers to install and configure them, particularly if the benefits of that flexibility are to be realised.[194] An analysis of recent research by Ofcom suggested that 83% of parents were aware of the existence of software to filter access to Internet content, but only 54% said that they had installed any.[195]

104. Filters to control access to Internet content using mobile phones operate at network level rather than being applied directly by consumers from handsets: an account holder simply specifies whether or not a handset may be used for access to adult content. Mobile network operators use age verification techniques to secure authority to lift blocks on access to adult content such as gambling, open chatrooms (those not hosted by network operators' portals) and games. Typically, those techniques will require users to submit credit card details or to present documents at an outlet of the relevant network operator.[196]

105. Mr Brennan, Parliamentary Under-Secretary of State at the Department for Children, Schools and Families, suggested that the mobile phone industry was in some senses leading the way in the protection of children from images which might be more easily accessible by other means, and he believed that they deserved credit for their approach.[197] Various factors combine to make network level filtering a viable proposition for access to the Internet through mobile devices: the market for filtering packages which can be installed locally on mobile devices is undeveloped; devices are usually used by one person rather than by several different family members, each of whom might need a different access

[190] Ev 380

[191] Ev 259

[192] Ev 43-44

[193] Ev 104

[194] Ofcom Ev 259

[195] Ev 231

[196] See for instance T-Mobile Ev 61, O2 Ev 67, Orange Ev 71

[197] Q 602

regime; and the volume of Internet traffic using mobile phones is much lower than for fixed Internet connectivity (using a PC).[198]

Age verification

106. Age verification is imperfect as a control. MySpace noted that there was no effective age verification mechanism "due to technical, legal and data challenges";[199] and Ofcom outlined three flaws:

- The difficulty of confirming age without a physical link: in Germany, access to regulated providers of online pornography is only granted upon production of identification at a post office, or a demonstration of identity via live webcam, or the physical receipt of a personal ID USB-chip. Requiring use of a credit card as proof of age is one solution but would exclude those who prefer to use debit cards (which are available to people aged under 18);[200]
- The cost to the provider of obtaining verifiable consent can be very expensive; and
- Placing the onus on the content provider to verify age may prompt providers to move to another jurisdiction where requirements are less onerous: anecdotal evidence suggests that registered providers of pornography to people in Germany had taken this step.

Nevertheless, Ofcom concluded that age verification, although not entirely secure, could help to control the availability of harmful content.[201]

107. The BBC requires children who sign up to use message boards on BBC websites to provide their date of birth; but it pointed out in its evidence to the Byron Review that "as there is no accessible national database we can use to check identity and age against, we are unable to confirm these ages, but we do all we can to keep the boards safe and age relevant". The BBC said that it would welcome "a pan-industry initiative to explore the feasibility of developing an age verification system that could "talk" to a secure and reliable database containing relevant children's personal information".[202] Dr Byron endorsed this proposal in her Report.[203]

Conclusions on access to potentially harmful content

108. There are many types of content on the Internet which are in most people's opinions distasteful or potentially harmful, but which are not illegal. Regulating access to such material largely depends largely on reports from consumers to site hosts and prompt action to take down content if it breaches Terms of Use or their equivalent.

---

[198] Ev 261

[199] Ev 150; also CHIS Ev 4

[200] Ev 255

[201] Ev 235

[202] Ev 377

[203] *Byron Review* paragraph 4.89

109. Internet service providers maintain that they should not police the Internet outside that part which they "own" and which is governed by their Terms and Conditions of Use. Google told us that it should not be the arbiter of what does and does not appear on the Internet, maintaining that this was a role for the courts and for the Government.[204] This position was supported by Dr Byron[205] and by mobile network operators, who pointed out that whereas they were free to impose conditions on the content hosted on their portals, they did not see it as their role to block access to sites which were hosted outside those boundaries. They maintained that it was the responsibility of consumers to decide whether or not they wished to retain the ability to view "legal but unpalatable" material.[206]

110. However, it should not be assumed that Internet service providers are opposed to tighter controls. Indeed, greater clarity about what is legal and what is not would be welcomed by some. Mr Galvin, representing BT, described the position in relation to possession of child abuse material as "unusually clear". He said that it "would be so much easier to produce a list" of sites featuring other types of potentially harmful content which should be blocked if the law were to be as clear in those areas. The Secretary-General of the Internet Service Providers Association stressed that the industry would welcome greater clarity, which would enable businesses to enforce their terms and conditions.[207] Dr Byron believed that the Government should define what was illegal and communicate that definition to ISPs.[208]

111. The Internet Watch Foundation pointed out that widening the blocking approach to other categories of material would not be easy: there was no common agreement about what might be blocked. For Internet service providers, the mechanics of imposing network level blocking to prevent access to pornography sites, of which there were "tens of thousands if not millions", would be a technical challenge and could slow down Internet traffic. However, the Foundation's Chief Executive, Mr Robbins, told us that "if there is a will, it can be done".[209] Orange, which is both a mobile network operator and an Internet service provider, agreed that the list of child abuse websites could serve as a model for other types of material if the Government were to deem it appropriate and provided that a list could be made available.[210]

112. Ofcom observed that the broad approach taken by the UK was replicated elsewhere but not necessarily as effectively, and it sketched the process by which access to illegal content is handled in Germany, where a blacklist of web addresses is compiled by Government agencies and by the Freiwilligen Selbstkontrolle Multimedia (FSM), a self-regulatory body. If illegal content is identified as being hosted in Germany, the host is issued with a take-down notice; if the content is hosted outside Germany, the address is notified to search providers, which will not provide links to the website on which the content is hosted. However, people in Germany may still be able to access the content if

[204] Ev 115

[205] Q 376

[206] Q 101 to 107

[207] Q 203

[208] Q 376

[209] Q 79 to 81

[210] Ev 69

they know the website address: in the UK this would be impossible, as access would be blocked by Internet service providers rather than by search providers.[211]

113. Not all witnesses favoured an approach which designates more types of content as illegal and which places an onus upon ISPs and others to prevent access once they become aware of such content. Professor Livingstone said that her understanding was that the industry was already making "all kinds of decisions about when to permit a certain kind of website to continue or to change the content" and that "all kinds of content regulation is going on under the banner of self-regulation". Her preference, rather than to designate more content as illegal would be to have "a more clear and transparent and coherent code" to manage content to make it difficult for a casual surfer to come across.[212] However, the dangers posed by some types of content arise not so much from casual or accidental access but through purposeful dissemination and incitement to illegal acts.

114. At a speech to the Convergence Think Tank on 11 June 2008, the Secretary of State for Culture, Media and Sport raised the question of whether standards applicable to traditional broadcast material might be applied in some way to online content. He appeared to take a view that they should be, saying "I worry that the online world will simply wash away all of the standards that have built up over time" and rejecting the view that standards have "no place online".[213]

115. There has been public alarm that Internet sites which provide information about committing suicide could be encouraging vulnerable people to commit self-harm or suicide and could have played a part in increasing the incidence of suicide in certain geographical areas.[214] Papyrus, a charity dedicated to the prevention of suicide by young people, told us that it had recorded 30 cases of suicide in the UK since 2001 in which the Internet had played a significant role by "providing detail of method and also direct encouragement through chatrooms". It drew our attention to two cases of "direct online promotion of suicide", including one in which a person died while filming himself online and being "encouraged" by a number of people.[215]

116. The Law Commission examined the treatment of assisting suicide in law in 2006 and concluded that the law offered an "adequate" solution to the problem. It found that, in the case of suicide websites, the act of publishing the website could be shown to constitute an offence contrary to the Criminal Attempts Act 1981, if the publisher had the requisite intention. Under section 1 of the Act, a person who intends to commit an offence and who does an act which is more than merely preparatory to the commission of that offence, is guilty of attempting to commit that offence.[216] The Commission also said that publication would be an offence under the Suicide Act 1961 if it could be shown that any single visitor to the website had been aided by the website to commit suicide.[217]

---

[211] Ev 262–3

[212] Q 33

[213] Speech available at www.culture.gov.uk

[214] HC Deb 7 February 2008 col. 1220

[215] Ev 399

[216] Section 1 of the Act defines the offences to which these provisions apply

[217] Inchoate Liability for Assisting and Encouraging Crime, Law Commission No. 300, Cm 6878

117. Mr Coaker, Parliamentary Under-Secretary of State at the Home Office, told us that "the Law Commission was clear that aiding and abetting suicide, whether it be online or offline, is illegal". He had a definite view on websites which encouraged or assisted suicide: "something should be done about it and it should be taken down.[218] Mr Wicks, Minister of State at the Department for Business and Enterprise, indicated in June 2008 that the Government was "deeply concerned" about suicide websites and that the Ministry of Justice was looking urgently at whether the law could be strengthened. An announcement is to be made shortly. **We await the announcement by the Ministry of Justice on whether the law might be strengthened to help prevent the use of the Internet to encourage suicide. Even if it concludes that the offence of assisting suicide is clear enough in law to enable successful prosecutions of those responsible for websites which assist or encourage suicide, we believe that the law should not be the only means of controlling access. The characteristics of the offence should be clear enough in law to enable access to such sites to be blocked on a voluntary basis, possibly through the procedures established by the Internet Watch Foundation. The UK Council for Child Internet Safety should accord a high priority in its work programme to discussions with the Ministry of Justice on whether the law on assisted suicide is worded clearly enough to include websites which encourage suicide and to enable action to be taken to block access to websites which assist or encourage suicide.**

118. While the Internet Watch Foundation has played a major part in protection from illegal and potentially harmful content, by notifying host sites in the UK that they should take down material, or by prompting Internet service providers to block access to sites hosted overseas, we received evidence warning strongly that this approach was seriously flawed. Dr Richard Clayton, a researcher in the Security Group of the Computer Laboratory at Cambridge University and author of several academic papers on methods for blocking access to Internet content, pointed out that there was no single blocking method which was both inexpensive and discerning enough to block access to only one part of a large website (such as FaceBook). In his view, the fatal flaw of all network-level blocking schemes was the ease with which they could be overcome, either by encrypting content or by the use of proxy services hosted outside the UK.[219] THUS plc, a provider of Internet services under the "Demon" brand in the UK, pointed out that the cost of implementing network-level blocking was "undoubtedly" passed on to consumers via service charges.[220]

119. Dr Clayton urged us to focus instead on blocking software installed and applied voluntarily by users. He observed that such software, while not perfect, could be customised and "should in principle be unaffected by the use of encryption or of proxy systems".[221] **At a time of rapid technological change, it is difficult to judge whether blocking access to Internet content at network level by Internet service providers is likely to become ineffective in the near future. However, this is not a reason for not doing so while it is still effective for the overwhelming majority of users.**

---

[218] Q 600

[219] Ev 368 to 370

[220] Ev 381

[221] Ev 370

120. The Child Exploitation and Online Protection Centre drew our attention to reports of simulated sexual activity with children on sites such as *Second Life*. Its Chief Executive Officer, Mr Gamble, believed that this was "absolutely" a matter which needed to be investigated: he reasoned that a person who wanted to engage in sexual activity with a child and was fantasising about it either in the real world or in a virtual one (such as *Second Life*), demonstrated a propensity for such an activity and posed a potential risk to children in real life.[222] Mr Lansman, the Secretary-General of the Internet Service Providers Association, clearly believed that regulation of the field was needed.[223]

121. We raised the matter with Ministers, who described the Government's consultation on the issue in 2007. Mr Coaker, Parliamentary Under-Secretary of State at the Home Office, pointed out that it would be a significant step for the law to intervene in an area when no-one had been harmed and no children were involved. He questioned whether, just because he might be disgusted and appalled if a paedophile were to use a site such as *Second Life* to create an avatar and to enact sexual abuse of children, such action should be made illegal. He noted disagreement about whether a person who acted out such a scenario in a virtual world would necessarily become more likely to do the same in the real world.[224]

122. Since Mr Coaker gave evidence, the Ministry of Justice has announced that it plans to bring forward proposals to create a new criminal offence of possession of drawings and computer-generated images of under-aged children in sexual activity. Maria Eagle MP, Parliamentary Under Secretary of State at the Ministry of Justice, described the proposals as "helping to close a loophole that we believe paedophiles are using to create images of child sexual abuse".[225]

123. Given the universal nature of the Internet and its characteristic of enabling access by a person in one country to a website hosted in any other country, access controls applied in isolation in one country, unless they are draconian, are going to be limited in effect. There is, however, no common view internationally on what material should be illegal and what is harmful; and there are no global standards. Action has been taken at European Union level, through the Safer Internet action plan and the Safer Internet *plus* programme, both of them initiatives lasting several years, to enable the establishment of a European network of hotlines for reporting illegal content, to provide information for parents through independent testing of the effectiveness of filtering software, and to support self-regulatory initiatives by the industry. A proposal has been drawn up for a further programme, with similar aims, to run from 2009 to 2013; this would (amongst other things) aim to reduce illegal online content.[226]

124. We have not been made aware of any other high-level international forum at which governments or regulators can share best practice or propose minimum standards for controls over access to content. It was pointed out to us that a large number of sites hosting material which would be illegal if hosted in the UK are based in the US, beyond the reach

[222] Q 174

[223] Q 201

[224] Q 600

[225] Ministry of Justice news release 28 May 2008

[226] See European Commission proposal, 29 February 2008, COM(2008) 106 final

of any EU initiative. **We believe that there would be advantage in establishing a forum at which governments or regulators from across the world could try to find common ground on how access to content on the Internet should be treated. This may, in time, lead to a more co-ordinated effort in frustrating access to material which is widely perceived as harmful. We recommend that the Government should take a lead in establishing such a forum.**

Controlling contact-based risks

125. The Home Office Taskforce on Child Protection on the Internet published good practice guidance for providers of social networking and other user interactive services in April 2008. As the Home Secretary notes in her foreword to the guidance, it was drawn up with considerable input from many of the main industry providers, some of which are based outside the UK. The guidelines set out extensive and detailed recommendations to service providers on how safety information should be made available to users, what steps should be taken when users register for a service, what tools users should be offered in maintaining their profiles, and how mechanisms for reporting abuse could best be structured. A further section offers safety tips to parents, carers, children and young people.

126. We discussed safety controls with operators of social networking services during oral evidence with Bebo and MySpace and during our visit to the United States, where we met representatives of Yahoo!, MySpace, Piczo and Facebook. Both Bebo and MySpace set minimum ages for use: 13 for Bebo and 14 for MySpace;[227] but it became clear during the inquiry that minimum ages are difficult to enforce. In order to track users who have lied about their age, MySpace and Bebo both use technology to search the site for terms commonly used by underage users.[228] Ofcom told us that social networking sites based in the United States had come under pressure from state Attorneys-General to take action of this sort.[229]

127. It is recognised good practice for social networking services to alert users to the risks of making public information about themselves, particularly information which can allow direct contact. Various forms of protection might be provided, such as:

- Reminding users that they are not anonymous online;
- Setting users' profiles to "private" by default for some or all users, thereby preventing access by people other than those specifically permitted: users can choose to remain private or opt to make their profiles public;
- Enabling users under 18 to block all contact from users over 18 (and *vice versa*); and

[227] Q 392 and Ev 150

[228] Ev 150 and Q 394

[229] Ev 257

- Enabling users to control who can see their individual photo albums and copy from them.[230]

Controls can also block the use of webcams, file transfer and access to chatrooms.[231] Professor Livingstone suggested that very often people were confused about how privacy controls on social networking sites work: she noted evidence that "people do not understand or do not take very seriously what those decisions [on privacy settings] are, partly because they are not aware of possible abuses of that information".[232]

128. **It is clear that many users of social networking sites, particularly children, do not realise that by posting information about themselves, they may be making it publicly available for all to see. We recommend that social networking sites should have a default setting restricting access and that users should be required to take a deliberate decision to make their personal information more widely available. We also recommend that consideration be given to alerting users through pop-up displays about the risks involved in submitting personal details without restricting access.**

"Report Abuse" buttons

129. As with sites which provide access to the open Internet, many providers of social networking services provide a Report Abuse button on each content page, enabling users to report to them concerns about inappropriate activity. Bebo provides a link to a Report Abuse form from each profile page; users can then report another user for inappropriate behaviour, in which case that user's profile will be reviewed by a moderator. Users can also submit a police report if they believe that a user is making inappropriate sexual comments: such reports are presently assessed first by Bebo's abuse management team before being forwarded (if the report is filed in the UK) to the Child Exploitation and Online Protection Centre (CEOP). Bebo told us in oral evidence that the turnround time was normally between one and four hours.[233] However, in response to a Parliamentary Question, CEOP undertook a sampling exercise to find out how much time elapsed between receipt of a report by Bebo and onward submission to CEOP. Using figures from the 2007-08 financial year, when Bebo submitted 290 reports of possible child exploitation to CEOP, the time period varied from seven hours to three days and 14 hours, with the average period being one day and 23 hours.[234]

130. MySpace also offers a facility for reporting abuse, although reports are forwarded automatically to the National Center for Missing and Exploited Children in the US before being referred to the appropriate law enforcement agency.[235]

131. Some interactive sites offer a direct "Report Abuse" link to the Child Exploitation and Online Protection Centre.[236] Mr Gamble, Chief Executive Officer of the Child Exploitation

[230] Bebo Ev 147, MySpace Ev 150

[231] See for instance BT memorandum Ev 103,Microsoft Ev 36

[232] Professor Livingstone Q 8

[233] Q 422 to 425

[234] HC Deb 20 May 2008, col. 225W

[235] Q 409

[236] See for instance Microsoft Windows Live Messenger Ev 36

and Online Protection Centre, described Microsoft Instant Messenger as being "one of the safest environments in the UK because you can report directly".[237] In the week after the direct report button in Microsoft Instant Messenger had gone live, the number of reports to CEOP increased by 113%; in the month that followed, the proportion of reports from people aged under 18 rose from 22% to 54%.[238]

132. We suggested to witnesses that there was, in certain cases, a need for users to be able to report potential abuse directly to law enforcement agencies rather than to site owners, which might take time to refer a report to an enforcement agency. Mr Walker, General Counsel for Google, speaking with reference to YouTube, said that he would be interested in talking further with CEOP about instituting a direct reporting system, although he said that "we have in many cases a global platform, so we need to find something that will work for law enforcement around the world". He said that he was "not in a position to commit to specific implementation at this point".[239] Bebo told us that it hoped to arrange for reports of abuse to be filed simultaneously to Bebo and to CEOP "in the near future".[240] We note that the Government would "definitely like to see progress" in this area.[241] **We commend Microsoft for providing a facility for direct reporting to the Child Exploitation and Online Protection Centre within Windows Live Messenger. We believe that high profile one-click facilities for reporting directly to law enforcement and support organisations are an essential feature of a safe networking site. We recommend that the UK Council for Child Internet Safety should impress upon providers of networking services the value of direct one-click reporting from their websites to law enforcement agencies and voluntary sector organisations with expertise in offering support to vulnerable people. We also believe that facilities for reporting abuse should be obvious to users and should be directly accessible from all relevant pages of a website, close to the entry point. We would expect providers of all Internet services based upon user participation to move towards these standards without delay.**

Moderation of interactive sites

133. Differing regimes exist for moderation of content in interactive sites. Dr Byron noted the importance of human moderation (as opposed to filtering tools or other technology) in sites designed for younger children, such as Club Penguin, or the BBC's CBeebies site, for which she believed the standard of moderation was "brilliant".[242] AOL, for instance, moderates all chatrooms which it operates for children.[243]

134. Users of social networking sites may be able to moderate some of the content on their sites. For instance, users can screen comments made by other users before allowing them

[237] Q 169

[238] Q 167

[239] Q 263

[240] Q 422

[241] Q 592

[242] Q 368

[243] Q 233

to appear on their own profile page; and they can delete comments posted by others on their page.[244]

135. Mobile network operators may exercise a fairly high degree of control over their customers' access to social networking sites and interactive sites which they host. Typically, chatrooms for under-18s and blogs are fully moderated.[245] T-Mobile told us that it moderated all interactive services hosted on its portal and that all images uploaded to social networking sites through that portal were moderated within two hours, and that key words in text content uploaded are detected and blocked. T-Mobile told us that it required providers of social networking services, as a minimum, to meet the standards set out in the Home Office Good Practice Guidance for providers of social networking and other user-interactive services published in April 2008; but it added that "although providers might be signatories to best practice guidance, in practice it is often difficult to negotiate safeguards in a contract or to fully understand what safeguards are operational, or even to include a specific notice and takedown provision".[246] We also note the statement by T-Mobile that takedown timescales varied greatly between different providers.[247]

Controlling conduct-based risks and cyberbullying

136. Attempts to prevent cyberbullying are largely co-ordinated by the Department for Children, Schools and Families (DCSF). Its predecessor, the Department for Education and Skills, published *Tackling Cyberbullying* guidelines in 2006; and the DCSF commissioned Childnet International to develop further guidance for inclusion in the department's main anti-bullying guidance for schools, issued in 2007.[248] DCSF has mounted a digital campaign, using interactive websites popular with children and young people, to increase awareness of the action which young people can take to minimise the risk of being cyberbullied. DCSF has also convened a Cyberbullying Taskforce, with representation from providers of Internet-based services, mobile phone companies, school staff unions, Becta,[249] children's charities and law enforcement agencies.[250]

137. T-Mobile told us that where cyber-bullying occurred, it provided practical advice, such as encouraging users not to reply to unwanted messages and not to delete them (as they could help to track an offender), and suggesting that parents involve the school in dealing with the problem. Most network operators have also set up help bureaux for customers who receive nuisance or malicious calls;[251] one solution can be to provide a change of phone number free of charge.[252] In some cases, culprits can be traced and

[244] Bebo Ev 147

[245] O2 Ev 69; T-Mobile Ev 62, Orange Ev 70.

[246] Ev 62

[247] Ev 64

[248] Ev 344

[249] Becta was formed in 1998 and describes itself as the Government's lead agency for Information and Communications Technology (ICT) in education in the United Kingdom.

[250] Ev 344

[251] Mr Bartholomew Q 119

[252] T-Mobile Ev 63, O2 Ev 66, Orange Ev 71

warned; O_2 told us that another option was to cut off customers found to be misusing their phones.[253]

138. We note that mobile phone call records would make it possible to establish that a particular phone had been used to upload content onto a video-sharing website at a particular time but would not necessarily identify the images uploaded or the person who had used the phone to upload them.[254] Given that images or videos taken by mobile devices may be uploaded to social networking sites or video sharing sites on impulse, it would seem important to be able to have a record of the nature of content handled, should it be offensive, harmful or even illegal. It may be that the mobile phone industry could develop technology which would allow images uploaded by mobile devices to be viewed, thereby helping in the process of assembling evidence if inappropriate conduct has taken place. **We recommend that network operators and manufacturers of mobile devices should assess whether it is technically possible to enable images sent from mobile devices to be traced and viewed by law enforcement officers with the appropriate authority.**

Limiting Internet use and game play

139. Another form of control of conduct-based risk is to use software to limit Internet use and game play, to counter any threat of "addiction" and to reduce scope for physical inactivity. Microsoft has developed a timer which will programme an Xbox games console to allow only specific amounts of playing time; after that time has expired, the child will not be able to use the console again within a 24-hour period without intervention by the parent.[255] Some governments have sought to introduce incentives to reduce the amount of time spent by players on video games, for instance by requiring or asking the industry to introduce high-scoring elements early in a game, with diminishing returns from prolonged play.[256]

140. **We commend Microsoft for their efforts to ensure that there are varied and effective parental controls built in to their hardware. We believe that other console manufacturers should be encouraged at least to match these. We hope that this matter will also be considered at an early date by the UK Council on Child Internet Safety.**

Merits of self-regulatory approach

141. Protection from potentially harmful content, contact and conduct on the Internet or using Internet-based services has rested until now largely with the industry, which has responded to varying degrees to the different types of threat. One of the questions central to this inquiry has been: is self-regulation by the industry succeeding?

142. Providers of Internet connectivity and of search services and social networking services spoke up strongly for what had been achieved so far through self-regulation. Mr Lansman, the Secretary-General of the Internet Service Providers Association, said that the

---

[253] Ev 66 and Q 119

[254] Q 126 to 132

[255] Ev 34. See also BT Ev 103

[256] Mr Carr Q 3, Ev 2

industry was "leading the way", and Mr Galvin, speaking on behalf of BT, said that self-regulation had given "a shining example of best practice in the best Internet service providers". Both Mr Lansman and Mr Galvin accepted that risks remained and would continue to emerge from new services.[257] Mr Walker, General Counsel for Google, said that the self-regulatory model for applying controls on access to Internet content had been "relatively successful", and he argued that "the risk of governmental or prescriptive rules being imposed on an industry which is effectively less than three years old runs a significant risk of unintended consequences".[258] MySpace believed that self-regulation was working well and was "the appropriate means to approach safety".[259] Bebo, while it expressed confidence in self-regulatory approaches, also accepted that the rapidly evolving nature of the market meant that businesses needed to review and improve their response continually.[260]

143. Mr Galvin also contrasted the self-regulatory approach with that of statutory regulation, saying that "I do not think you would have seen the pace of our co-operation with legislation, because inevitably it goes more slowly".[261] He did not, however, discount the need for statutory regulation, to determine where the line between illegal and harmful or unpleasant content should be drawn.[262]

144. Some of the industry's efforts in self-regulation have been much praised and admired. The Internet Watch Foundation said that it was "consistently referenced as a national and international model of effective self- and co-regulation" and was recognised as an influential and relevant authority by many sectors.[263] Others also spoke highly of the Foundation's work.[264] The Child Exploitation and Online Protection Centre applauded the work of the Foundation and also described the Clean Feed[265] system operated by BT as "an outstanding, world-leading initiative".[266]

145. We note that 95% of domestic broadband consumers buy Internet access from about seven companies, all of which apply the IWF list. The remaining 5% use a "tail" of perhaps 100 companies some of which do not block access, although some of those may in fact be reselling internet connectivity from larger companies who have already imposed the blocks. The Internet Watch Foundation told us that it believed that there were "issues … in relation to cost and effectiveness" underlying the reluctance of smaller ISPs to block access.[267]

---

[257] Q 252

[258] Q 269

[259] Q 431

[260] Ev 147

[261] Q 201

[262] Q 253

[263] Ev 46

[264] ISPA Ev 101; Dr Byron Q 337

[265] Filtering software used by British Telecom to block access to child pornography websites

[266] Q 168

[267] Q 55 to 57

146. The Internet Service Providers Association said that it encouraged as many Internet service providers as possible to apply the Foundation's list.[268] The Home Office set a target for all ISPs to agree by the end of 2007 to block access to sites on the list: when we raised the issue in oral evidence in May 2008, it was plain that little progress had been made in persuading the remaining 5% to act. Ministers appeared to be losing patience and were considering their options, which include legislation.[269] **We expect the Government to apply continuing, and if necessary, escalating pressure on Internet service providers who are showing reluctance to block access to illegal content hosted abroad. In a lucrative market, the cost to Internet service providers of installing software to block access to child pornography sites should not come second to child safety.**

147. Although most witnesses were complimentary about the efforts of the industry, we were struck by the considerable anxiety expressed by the Chief Executive of Ofcom about the effectiveness of self-regulation as presently operated. He believed that current arrangements "cannot persist" and was particularly critical of the lack of clarity about take-down procedures and the lack of transparency about complaints. In his view, "we do not have anything even approaching an effective self-regulatory model for this". He set a timescale of 12 months for Internet-based industries to "come closer to the broadcast world": for him, the test was: would the industry "step up to the plate"?[270] He did not, however, believe that there was a clear case for Ofcom to acquire more regulatory powers in relation to the Internet, or at least not yet. He maintained that Ofcom's instinct "has always been and remains to regulate in the least intrusive, least bureaucratic way possible", and he was satisfied that there was "a real opportunity for self-regulation to be effective".[271]

148. The Child Exploitation and Online Protection Centre, in its submission to the Byron Review, proposed that there should be "a critical examination of whether the voluntary, self-regulation approach to protecting children and young people works effectively as it stands and actually delivers real and tangible change when it comes to the protection of children, whether it is sustainable in the long-term as new providers come on stream and actually delivers change, including the need to monitor the implementation of good practice guidance by service providers".[272] The Centre's Chief Executive Officer, Mr Gamble, claimed that some elements in the Internet services industry were "difficult", avoided engagement with CEOP, and were unwilling to co-operate with CEOP in its efforts to protect young people from harm.[273]

149. Childnet International, a charity which seeks to improve the safety of children using the Internet, told us that it accepted the importance of self-regulation to the Internet industry and said that it would be "hesitant" to propose stringent regulation.[274] It described the self-regulatory regime set out under the Communications Act 2003 as being widely considered as successful; but it regretted that compliance with that regime was not

[268] Q 202

[269] Q 612-3

[270] Q 512

[271] Q 517

[272] Ev 87

[273] Q 187 and 189

[274] Ev 12

monitored. It spoke of the "valuable guidance" drawn up in best practice guidelines set out by the Home Office Taskforce and through best practice guidance drawn up by industry bodies such as the Internet Service Providers Association; but adherence was not mandatory and it believed that there was no way to verify easily how far the industry was conforming to its own guidelines.[275] Professor Livingstone suggested that an independent body might be established to oversee and report on the effectiveness and the accountability of self-regulatory codes.[276] Dr Byron took much the same view, suggesting that the industry should set out "very clear safety codes and general good practice principles" which could then be independently monitored and evaluated.[277]

150. There are signs that the Government expects the industry to take a stronger line. For instance, in an Adjournment debate on cyberbullying on 20 February 2008, the Rt Hon Beverley Hughes MP, Minister of State at the Department for Children, Schools and Families, said that "we need business to raise its game" in preventing cyber-bullying.[278] We asked Ministers to offer their views on whether the time had come to establish a body to oversee Internet standards, in the manner of the Advertising Standards Authority or the Press Complaints Commission. The Rt Hon Margaret Hodge MP, Minister of State at the Department for Culture, Media and Sport, said that "we always keep an open mind" but that, at present, the Government did not want to over-regulate: rather, it would prefer to work through voluntary mechanisms and existing structures. She said that the Convergence Think Tank was considering the issue.[279]

151. There appear to be conflicting views within the industry on the practicality of applying certain standards. Divergences in practice are especially noticeable in the allocation of resources by Internet-based services to pro-active screening on sites hosting user-generated content and the provision of facilities to report directly to law enforcement agencies. Many companies publish their own codes and policies for child protection but there are significant variations between these. We also note that, if a company's practice is poor, there is no independent body to which a user might submit a complaint and no body to enforce minimum standards. We note with interest research conducted by Ofcom suggesting considerable uncertainty among parents about who to complain to if they discovered potentially harmful or inappropriate content online. Approximately one-third of the sample said that they would complain to the police; 14% would complain to their Internet service provider; 11% would complain to the website itself; and almost four out of ten did not know who they would complain to.[280] Mr MacLeod, Chair of the Mobile Broadband Group, listed various channels by which complaints about content access through mobile devices were received: through Ofcom, the Independent Mobile

[275] Ev 12

[276] Q 34-35

[277] Q 349

[278] HC Deb 20 February 2008 col.493

[279] Q 607. The Convergence Think Tank was set up jointly by the Department for Culture, Media and Sport and the Department for Business, Enterprise and Regulatory Reform to examine the implications of technological development for the media and communications industries, and the consequences for both markets and consumers.

[280] Ev 211

Classification Body, the Mobile Broadband Group and the network operators themselves.[281]

152. This Committee has broadly been a supporter of self-regulation in various fields, such as regulation of on-demand broadcast services, the secondary ticketing market and press standards. We recognise that self-regulation has a range of strengths: a self-regulating industry is better placed to respond quickly to new services; it is more likely to secure "buy in" to principles;[282] and it will bear the immediate cost. We accept that a great deal has been achieved through self-regulation by the various industries offering Internet-based services, but there appears to be too great a disparity in practice between different firms and not enough evidence that standards of good practice are being consistently followed.

153. **We believe that leaving individual companies in the Internet services sector to regulate themselves in the protection of users from potential harm has resulted in a piecemeal approach which we find unsatisfactory. Different practices are being followed and there is a lack of consistency and transparency, leading to confusion among users. Nor is there any external mechanism for complaints about services provided by Internet-based industries to be considered by an independent body. However, we do not believe that statutory regulation should be the first resort. Instead, we propose a tighter form of self-regulation, applied across the industry and led by the industry. We therefore call on the industry to establish a self-regulatory body which would agree minimum standards based upon the recommendations of the UK Council for Child Internet Safety, monitor their effectiveness, publish performance statistics and adjudicate on complaints.**

154. **We recognise that a number of companies may choose to set higher standards for their own commercial reasons, but the public need the assurance that certain basic standards will be met. This is particularly important in the area of child protection and Internet safety. However, the new body might also take on the task of setting rules governing practice in other areas such as on-line piracy and peer to peer file-sharing, and behavioural advertising, which although outside the scope of this inquiry are also of public concern. Given the global nature of the industry, it is impossible to make membership compulsory for all service providers, but a widespread publicity campaign should ensure that consumers are aware that they can have confidence in the standards of protection and reputable practice which membership of the body carries with it and that this cannot be guaranteed by those companies that choose not to join.**

155. We considered whether the UK Council for Child Internet Safety should, in time, take on a wider role in leading self-regulation of Internet service industries. Our conclusion is that this would be inappropriate, as the Council has been established as a forum in which Government departments, the industry and relevant voluntary sector bodies can work together in developing a strategy for child Internet safety. Its role should be to agree on recommendations of minimum standards for the industry to meet. The implementation and enforcement of these would be the responsibility of the self-regulatory body. In this respect, the UK Council would have a similar role to the Committee of Advertising

[281] Q 145

[282] See T–Mobile Ev 61

Practice which draws up the Code governing the non-broadcast advertising industry. The Code is then enforced by the Advertising Standards Authority Council, which has a mixed membership from the industry and from the voluntary sector, with no presence from either the Government or from Ofcom. **Our preferred model for any new body to maintain standards among providers of Internet-based services is that of the Advertising Standards Authority, which is generally successful at securing compliance with codes for advertising standards but which, if necessary, may refer companies which persistently breach those standards to statutory regulators that can apply penalties.**

The role of Government

156. Although we have identified a role for the Government in bringing forward legislation to define certain types of content on the Internet as illegal, we do not believe that, in general, this is a field in which the Government should be very closely involved. Its chief role should be to ensure that bodies with a regulatory, advisory or law enforcement role in protection from harmful content on the Internet and in video games have priorities which are in line with Government policy and are resourced to carry out their duties effectively.

157. The Government has performed a service by bringing the issue of protection from harm on the Internet to the fore. The creation of the Home Secretary's Taskforce on Child Protection on the Internet and, more recently, the Child Exploitation and Online Protection Centre, signalled how seriously the Government took the protection of children from risks from the Internet. Commissioning the Byron Review was another big step forward. **We commend the Government for the action it has taken to motivate the Internet industry, the voluntary sector and others to work together to improve the level of protection from risks from the Internet, particularly for children. However, we regret that much of this work remains unknown and has therefore done little to increase public confidence. We look to the UK Council to build on the existing agreements and to ensure a much greater public awareness of what has already been achieved.**

158. We note criticism that the Government has not been "joined up" in its approach.[283] This is an easy criticism to make but a difficult one to refute, especially in an area where so many Departments have an interest. For instance, the Department for Children, Schools and Families has policy responsibility for schools, which have a role in educating children in safe use of information technology and the Internet; the Department for Culture, Media and Sport has an interest in the Internet as a medium through which creative content is disseminated; the Home Office has a role in the protection of the public and in law enforcement; and the Department for Business and Enterprise has responsibilities for the regulatory structure within which Internet-based services operate, including regulation based upon the E-Commerce Directive. The Ministry of Justice has taken the lead in policy on possession of computer-generated images of under-aged children in sexual activity.

[283] *Byron Review* paragraph 3.112

159. Ministers sought to persuade us that the Government was "very joined up" in its approach to the matters considered by this inquiry.[284] Certainly, there have been good examples of cross-Departmental collaboration, for instance in the establishment of the Byron Review. However, we recall Dr Byron's statement that the Internet industry was "very fatigued" at dealing with different Government departments which, individually, were having "several sometimes contradictory conversations" with the industry.[285] **We also note that the Government originally suggested that four different Ministers should give evidence to our inquiry and it does seem that there is scope for improved co-ordination of activity between different Government departments. We recommend that a single Minister should have responsibility for co-ordinating the Government's effort in improving levels of protection from harm from the Internet, overseeing complementary initiatives led by different Government departments, and monitoring the resourcing of relevant Government-funded bodies.**

5 Media literacy

Why media literacy matters

160. Many of the controls described earlier in this Report, such as filter settings and privacy settings for social networking profiles, are designed to be applied by consumers, at their discretion. Such controls can only be effective if consumers understand what choices they have, and the evidence to this inquiry has suggested that many consumers are either unsure of what is being offered and what their choices are or they are unaware of why those choices matter.

161. The understanding needed to make those informed choices underlies the term 'media literacy',[286] enshrined in section 11 of the Communications Act 2003, which places upon Ofcom duties to bring about (or encourage others to bring about) better public understanding and awareness of aspects of material published using electronic media. Ofcom told us that it did "absolutely everything we can" to carry out that duty: it would spend more than double what it would receive in Grant in Aid in 2008-09 because of the priority which the Ofcom Board accorded to it. Ofcom sees its role as an enabler, not, for instance delivering information campaigns but rather helping in the co-ordination and promotion of initiatives.[287]

162. The need for greater awareness of the risks and the ways in which they might be controlled was widely recognised in evidence and was one of the main themes of the Byron Review.

[284] Mrs Hodge Q 578

[285] Q 347

[286] See also UK Film Council submission, Ev 47

[287] Q 522

Steps taken to raise awareness

163. It was put to us that manufacturers and retailers selling Internet-enabled devices for the domestic market did "not routinely provide any safety-related advice about the technology".[288] Some believe that hardware manufacturers and retailers have shirked their duty to inform consumers: the Children's Charities' Coalition on Internet Safety (CHIS) criticised what it saw as manufacturers' and retailers' reliance upon parents to take the initiative in buying and installing safety software.[289] We also note the observation by the House of Lords Select Committee on Science and Technology, in its inquiry into Personal Internet Security, that "the current assumption that end-users should be responsible for security is inefficient and unrealistic".[290] Witnesses representing Internet-based services, on the other hand, drew attention to the comprehensive safety information which they placed on their websites.[291]

164. The Children's Charities' Coalition for Internet Safety criticised the Internet industry for failing to match expenditure on advertising products with expenditure on child protection.[292] We asked witnesses from the industry about their budgets for child protection in the UK, but few were able to give us figures. BT suggested that it spent £1 million, "possibly more".[293] AOL said that "we do not have a figure because it is integrated in any of our products".[294] Neither Bebo nor MySpace were able to give us definitive figures for the UK in oral evidence, pointing out that there was no distinct safety budget,[295] or that safety efforts "were on a global basis" and could not be broken down by country,[296] or that spending on safety was difficult to identify as it was integral to the company.[297] MySpace subsequently provided us with a figure for its overall annual safety budget, and Google provided a figure for spending in the UK on online child protection. Both of these figures we have treated in confidence, as requested.

165. We note that mobile network operators have created a dedicated website for teachers, offering information and advice on how to manage issues associated with misuse of mobile phones.[298] The Government and the Internet industry have jointly sponsored the *Get Safe Online* campaign, designed to educate users on how to protect themselves online and to make people aware of the treats to their personal security.[299]

---

[288] Ev 6

[289] Ev 6, Q 32

[290] Fifth Report of the House of Lords Committee on Science and Technology: *Personal Internet Security,* HL 165-I, Session 2006-07, paragraph 3.67

[291] For instance Microsoft on the MSN site Ev 39, T-Mobile Ev 63, O2 Ev 67, Orange Ev 71, MySpace Ev 152

[292] Ev 7

[293] Q 212

[294] Q 216 to 219

[295] MySpace Q 396

[296] MySpace Q 395

[297] Bebo Q 407

[298] Ev 67

[299] Internet Service Providers Association Ev 99

166. The information provided by much of the industry is complemented by leaflets, websites and campaigns mounted by the voluntary sector. A CD on child internet safety produced by Childnet International—Know IT All for Parents—has been made available to all maintained schools in England free of charge: over one million orders were received within a few months.[300] Childnet International cited O_2 as a network operator which had agreed to use a checklist drawn up by Childnet, in its communications with customers, prompting parents with questions that they should ask mobile operators in order to ensure that available protective measures were in place on their child's phone.[301] BT listed many other sites offering safety advice, including Parentscentre.gov.uk, Kidsmart.org.uk, Getnetwise.org, Besafeonline.org and Saferinternet.org.[302]

167. Jim Gamble, Chief Executive Officer of the Child Exploitation and Online Protection Centre (CEOP), reminded us of the educational work undertaken by the Centre, complementing its law enforcement activities. The Centre has launched a national campaign—Think U Know—providing advice on how to have fun online, how to stay in control online, and how to report online. Since July 2006, CEOP has trained over 4,000 school liaison officers, educational professionals and local safeguarding children board members in the programme. Mr Gamble told us that "we want to make sure that our education programme goes to every single child in the country, not just the ones in mainstream schooling but those who are vulnerable and harder to reach".[303] CEOP has also established a Youth Advisory Panel, composed of 60 children aged between 11 and 16 "working to help us ensure that all our resources and messaging remain contemporary, engaging and clear".[304] CEOP's efforts in this area have been impressive, and we believe that it should have the resources to continue to fund this work.

168. The wealth of information available to consumers in the UK may be almost overwhelming. BT accepted that all such sites appeared to provide good advice, even if they took different approaches, but it argued that "what is missing is an overall campaign that pulls all of the initiatives together"; and other witnesses agreed.[305] Mr Lansman, Secretary-General of the Internet Service Providers Association, pointed out that information needed to be available in hard copy format, which would be more likely to be read by parents than online information.[306]

169. Several witnesses questioned how extensively filters were understood and used. Microsoft accepted that some of the tools which it offered to parents to filter harmful content were not very widely used, though this did not necessarily mean that there was low awareness.[307] Childnet believed that there were still parents who were not aware of the tools

[300] Ev 12

[301] Ev 12

[302] Ev 104. See also Ofcom Ev 264

[303] Q 183

[304] CEOP Annual Review 2007-08, page 20

[305] Ev 104. See also Q 73 and 74; ISPA Ev 100

[306] Q 255

[307] Q 46

available, did not know how to use them or deactivated them because they blocked too much material.[308]

170. BT disputed claims that uptake of parental controls was low. It observed that less than one third of UK households had dependent children and concluded that it had to be borne in mind, when dealing with figures for take-up of controls, that two thirds of households did not have dependent children. BT estimates that 42% of its broadband customers that have children aged between 5 and 15 have in fact set up parental controls.[309]

171. The Australian Federal Government, in an attempt to increase general awareness of the value of filtering tools, used public funding to offer a filtered service or a free filter for home computers, either for download from a dedicated website or supplied on CD. Internet service providers were also required to offer filters to new and existing customers at no additional cost.[310]

172. We also note the opinions of Professor Livingstone and Ms Millwood Hargrave that there is as yet little evidence that efforts to raise awareness have been effective in the extent or nature of risk or in affecting how children respond to risk. They concluded that while it seems likely that awareness and increased media literacy have a positive role to play in the management of content-related risks, more research in the area—and on what worked best—was urgently needed.[311]

173. Other tools, besides filtering, are being developed for use by parents or carers in controlling children's Internet access. Using Microsoft's Family Safety Settings, parents can generate activity reports for each family user, chronicling their children's Web browsing and online communication history.[312] MySpace told us that it was developing software which, once downloaded onto a PC, would reveal information which had been provided by users (such as age, user name and home town). Parents could then establish whether their child had a MySpace profile and, if so, what age they had claimed to be, regardless of the computer subsequently used by that child to log into the MySpace site.[313]

174. Childnet International told us that it firmly believed that the "key universal point of access in engaging with children, young people and schools in managing the potential and actual risks of engaging with the Internet is through schools".[314] The Children's Charities' Coalition for Internet Safety (CHIS) recommended that Internet safety skills should be a part of the PSHE element of the national curriculum,[315] although it argued that to rely solely upon schools as the vehicle to reach parents would not be sufficient, as "some of the most vulnerable children and parents will have little contact with school".[316]

---

[308] Ev 12

[309] Ev 103

[310] Childnet Ev 12 and Ofcom Ev 259

[311] Ev 18

[312] Ev 36

[313] Ev 151

[314] Ev 11

[315] Ev 7

[316] Ev 5

The role of parents

175. The Children's Charities' Coalition for Internet Safety told us that "in our experience, it tends to be that the majority of parents have a poor understanding of what children are actually doing online and an even poorer understanding of how to protect them in that space".[317] It commented on "the overwhelming gap between what parents know and what children know in terms of the technical aspects of IT"; and it recommended "a major public awareness campaign that educates adults and children about Internet safety". Ofcom's survey of children, young people and online content, published in October 2007, recorded high levels of concern among parents about Internet content but an alarming lack of knowledge about where to find information to help them protect their children online: 57% of parents said that they did not know where to find such material.[318]

176. Dr Byron told us that she had been struck by how people were not warning their children about the dangers of contact on the Internet because they were unaware of what their children were doing while they were online. She said that "a lot of people think when their kids are going online that they are watching television and so the Internet is used as an electronic nanny. It is not: it is actually like opening your front door and saying "Go on then, go and play"".[319] Mr Gamble, Chief Executive Officer of the Child Exploitation and Online Protection Centre (CEOP), pursued a similar point: he observed that a parent who allowed a child to enter a shopping mall would first warn and educate that child about the dangers. He said that parents had "a responsibility with regard to how you empower young people with information which makes them safe"; he argued that the same responsibility applied in the online environment as in the offline one.[320]

177. Yet parents can be unduly relaxed about their children's activities on the Internet or when playing video games. Professor Livingstone spoke of "a kind of casualness within the home or a difficulty for parents" in regulating game-playing.[321] Microsoft told us that parents tended to allow their children more freedom in the online world than in the offline world: for example, they would allow their children to play a computer game rated as suitable only for older children but would not allow their children to watch a film with such a rating.[322] One witness told us of research suggesting that although the large majority of parents were aware of the existence of an age-related video rating system, they did not always operate it, possibly because they had not played video games themselves when children and were not familiar with the type of content.[323] Dr Byron had herself witnessed an adult buying a classified game for a child, reasoning that it was "only a game".[324]

178. Ofcom, in support of its submission to the Byron Review, conducted a survey of research into Internet use and safety. It found that:

---

[317] Ev 5

[318] Ev 234; see also Q 535

[319] Q 337

[320] Q 167

[321] Q 3

[322] Ev 31

[323] Q 51

[324] Q 346

> "while many parents seem to have a good understanding of what their child uses the Internet for at home, there are some notable exceptions: they seem to be underestimating, in particular, game playing, watching video clips, using social networking sites and contributing comments to someone else's webpage … Around one in five parents do not know if their child has a social networking site profile".[325]

Parents also appeared not to be fully aware of their children's exposure to potentially harmful or inappropriate content when away from home, particularly when accessing the Internet at friends' or relatives' houses.[326] The research exposed discrepancies between parents' perceptions of their children's Internet use and children's accounts of their use: it would appear that parents often believe that their child does not have a social networking profile or has not viewed sites featuring user-generated content when the child claims that in fact they do have a profile or have viewed such content.[327] Alternatively, parents may not appreciate fully the reach of sites hosting user-generated content: a Minister told us of his surprise at finding that one of his daughter's videos on YouTube had been viewed by over 100,000 people.[328] Recent research commissioned by Orange found that 65 per cent of parents aged 41-60 had never accessed a social networking site while 65 per cent of under 16s use social networking sites at least once a week.

179. Childnet International warned that parents' ignorance of the potential harm could isolate a child, who might choose not to confide in a parent who it perceived as being ill-equipped to give advice. It also noted that young people might fear that the parent or carer would respond by confiscating their mobile phone or limiting their Internet access.[329] Microsoft told us that it advised parents to "make it clear from the moment you give your child online access that it will never be taken away because of them reporting inappropriate or offensive behaviour", and it observed that only 17% of children who had been victims of cyberbullying had told their parents, precisely because they feared having their Internet access taken away.[330] Dr O'Connell, Chief Safety Officer at Bebo, reinforced this point.[331]

180. Ofcom clearly believes that responsibility will rest increasingly with parents. When we discussed with Ed Richards, Chief Executive Officer at Ofcom, how a regulatory framework might control access to content when technology was enabling access on demand to material beyond jurisdictional reach or was eroding the relevance of established controls such as the nine o'clock watershed for television broadcasts, Mr Richards replied: "Is it possible for parents to police the access of their children to certain content by using that software or that hardware in a particular way? I think in all honesty that is the territory we are heading into. It is very difficult to imagine us regulating the broadcast stream in a

[325] Ev 191

[326] Ev 210

[327] Ev 219 and 220

[328] Q 623

[329] Ev 11. See also submission from Professor Livingstone and Ms Millwood Hargrave Ev 17, Mr Carrick-Davies Q 20

[330] Ev 39

[331] Q 388

particular different way unless we were to say that we are now going to stop certain content even after nine o'clock, which is almost unimaginable".[332]

181. Ms Church, Mobile and Broadband Safety Services Manager at Orange UK, told us that a child needed to be able to cope with the risks of the real world and that "there is no substitute for a parent sitting down, discussing what is safe and responsible use and ensuring complete understanding of what the risks are on the Internet.[333] When we raised with Mr Purvis, the Partner for Content and Standards at Ofcom, the question of how to control children's access to adult content which could now be downloaded on demand at any time of day, he pointed out that parents had a responsibility to use the tools available to control access: "parents have not shirked it over sending them to bed at nine o'clock so why somehow should it be thought acceptable for parents to shirk the responsibilities in an online area"?[334]

182. In the past, parents have been able to exercise some control, if they chose, over their children's Internet access, by siting home computers in a communal area such as the living-room, rather than in a child's bedroom. While this remains a sound principle—and there are particular dangers in siting webcams in children's bedrooms—it is of less value now that children often access the Internet through portable devices such as laptops or mobile phones, which allow unsupervised access. Mr Bartholomew, Head of Public Affairs at O_2, pointed out that there were now other types of device (such as the iPod touch and the Sony PSP) which allowed Internet access while "on the move"; none of these used the mobile phone network and they thereby fell outside content regulation structures built up by the network operators.[335]

183. Dr Byron examined in great detail the scope for improving children's and parents' media literacy. Her recommendations included a "properly funded education and public information and awareness campaign on child internet safety", a "one-stop shop" for child Internet safety within the DirectGov information network, and more stress upon e-safety in schools and on teacher training programmes. She also urged better use by parents of parental control software and safe search settings on computers used at home.[336]

184. The Children's Charities' Coalition on Internet Safety proposed that computer hardware supplied for home use should have child safety software installed and set to the highest level of security.[337] Although Dr Byron accepted the case for the supply of hardware with safety software already installed, she did not agree that it should be set to the highest level: she believed that it would be more valuable to require users to make a decision, when setting up the hardware, on what level of filtering they would choose to apply. She also suggested that users could find the highest level of filtering so restrictive that they simply switched it off altogether.[338] Microsoft suggested that consumers might become so

[332] Q 507

[333] Q 117

[334] Q 520

[335] Q 136

[336] *Byron Review* paragraph 4.74 and much of chapter 5, for instance paragraphs 5.46 and 5.73

[337] Q 32

[338] Q 377

frustrated that they would migrate to a different technology which enabled more open and uncontrolled access to inappropriate content.[339]

185. **We endorse the thrust of Dr Byron's recommendations on improving media literacy, and we commend her for her approach. However, we believe that the one-stop shop will only be worth locating on the DirectGov website if search tools, social networking sites, video-sharing sites and Internet service providers offer a direct link: otherwise the one-stop shop will languish in obscurity. We also recommend that all new computer equipment sold for home use should be supplied with a standard information leaflet, to be agreed with the IT hardware and software industries through the UK Council on Child Internet Safety, containing advice for parents on Internet safety tools and practices.**

186. **We agree with Ofcom that parents will need to take on greater responsibility for protecting children from harm from the Internet and from video games. In particular, they should be aware of the consequences of buying devices which allow unsupervised access to the Internet; they should have more knowledge of young children's social networking activities and be more familiar with video game content, thereby gaining a better understanding of the risks; and they should, wherever possible, discuss those risks openly with their children. We recommend that the UK Council for Child Internet Safety should investigate ways of communicating these messages to parents.**

6 Classification of video games

187. Many video games—particularly those which are console based or which are supplied on DVD or other similar formats—fall within the definition of "video work" in the Video Recordings Act 1984,[340] in which case their sale and distribution will be subject to controls under the Act if the game depicts:

- human sexual activity or acts of force or restraint associated with such activity;
- mutilation or torture of, or other acts of gross violence towards, humans or animals;
- human genital organs or human urinary or excretory functions

or if it is designed to stimulate or encourage either of the first two types of activity. Games which include clips from films will automatically be subject to classification. Online games, where the software is hosted on a website rather than on a consumer device, and which are played via a live Internet link, are not covered under the Act.[341]

188. It is illegal to supply any non-exempt video game[342] without a classification or in breach of a classification. Non-exempt games are therefore submitted to the British Board of Film Classification (BBFC), as the authority designated by the Secretary of State; once

[339] Q 52

[340] Any series of visual images (with or without sound) produced electronically by the use of information contained on any disc or magnetic tape and shown as a moving picture.

[341] BBFC Ev 294

[342] Any game depicting activities or characteristics listed in paragraph 187

classified, a video game may be marketed within the constraints imposed by the BBFC's classification.

189. Most video games do not require classification. In 2007, 101 out of the 1231 video games released into the UK market were submitted to the BBFC for classification either because they were judged by the games' publishers to be non-exempt under the 1984 Act or because they contained film clips. Of these 101 games, 29 were classified as being suitable only for players aged 18 or above, 19 games were classified as being suitable only for players aged 15 and above, and 2 games were classified as being suitable only for players aged 12 and above. Only 2.4% of the 1231 games released in 2007, therefore, received an "18" certificate.

190. Up to twelve examiners employed by the BBFC may be called upon to examine video games submitted for classification. Examiners play the games, typically for around five hours, although some games may take less time to examine and others more: *Manhunt 2*, for example, took a total of more than 100 examining hours.[343] The BBFC currently classifies around 250 video games each year and envisages "an increase of 300-500 games per year" initially. Currently, the BBFC classifies a game within ten days.[344] The classifications awarded are the same as those for films.

The PEGI system

191. The video games industry in the UK has operated its own ratings system for video games since 1994. Since 2003, the ratings used have been those of the PEGI (Pan-European Game Information) system, established by the Interactive Software Federation of Europe, and now used in 28 European countries.[345] PEGI ratings are awarded in the UK by the Video Standards Council (VSC), a non-profit making body established in 1989 at the request of the Government "to develop and oversee a code of practice designed to promote high standards within the video and video games industries".[346]

192. PEGI is a voluntary age rating system, based on self assessment by games publishers, who complete an online questionnaire giving "yes" or "no" answers to a "series of carefully worded questions relating to the content of the game".[347] The PEGI system then specifies a provisional age rating. If a game is assessed as being suitable only for players over 16 or over 18, it is submitted to the Video Standards Council, whose examiners will play the game for an average of two to three hours to assess whether the publisher's assessment is correct. A game's PEGI rating may be displayed on its packaging, as may a pictogram further outlining the nature of the game's content. There are seven pictograms symbolising violence, sex/nudity, drugs, bad language, gambling, material which may be "scary for young children" or "material which may encourage discrimination".[348]

---

[343] Ev 338

[344] Information supplied by BBFC

[345] A trade body

[346] Ev 323

[347] Ev 324

[348] http://www.pegi.info/en/index/id/175

Online games

193. Over time it is likely that more and more games will be distributed on-line. Although it is not a legal requirement, the BBFC now offers online distributors the opportunity to have their games classified by BBFC.online. The scheme offers members online classifications where a work has been granted a Video Recordings Act certificate with point of sale information using the recognised BBFC branding. Many games are classified by "PEGI Online", an offshoot of the PEGI system. The same process of self-assessment and (if necessary) verification by the Video Standards Council is followed; and the same ratings system is used. Games publishers which submit games to PEGI Online for classification may display the PEGI Online label on their websites. We note that mass-market games consoles, such as Xbox, Playstation and Wii, only permit access to games sites that have been approved by PEGI Online. Consumers may also use filtering software to block access to games on websites not approved by PEGI; but we were told that some filters could not currently discriminate between sites approved by PEGI and those that are not. More sophisticated filtering software is being developed.[349]

The hybrid system proposed by Dr Byron

194. For many video games available for sale in the UK, therefore, two classification systems are running side by side. It was suggested to us that the dual system was confusing for parents and retailers,[350] and Dr Byron considered the issue in her Review. She recommended that the two classification systems should be streamlined into one hybrid system, which should be extended to require classification of all games containing content which would presently receive a 12+ PEGI rating, to be underpinned by the statutory controls on supply established under the Video Recordings Act 1984. Under Dr Byron's proposed hybrid system, BBFC logos and classification codes would be on the front of all games packaging, and PEGI would continue to award ratings to games with content suitable for children aged under 12.

195. Dr Byron envisaged that the BBFC and PEGI would need to work together to align the criteria underlying such games for which, in effect, classification would be undertaken by PEGI using BBFC symbols. This proposal has provoked some anxiety in the BBFC. The Board's Director, David Cooke, said in evidence that "we are always nervous about the idea of putting our symbols to a methodology that we are not ourselves operating".[351] However, the BBFC has indicated that it would be willing to accept the proposal provided that it is able to check the classification methods used.

196. The Government has pledged to implement all of Dr Byron's recommendations, although it has recognised the controversy generated by her proposals for games classification and has agreed to consult on them with the games industry and parents. The Byron Review Action Plan, published in June 2008, announced that the Government would launch a four month consultation on reforming the classification system for video

[349] Ev 337

[350] British Board of Film Classification Ev 301, Entertainment Retailers Association Ev 365

[351] Q 543

games in July 2008 and would publish proposals for reform by early 2009. A full assessment of the costs to the industry of reform will also be carried out.[352]

197. We held oral evidence sessions with games developers, games publishers and bodies with a role in games classification, in each case after the publication of Dr Byron's Report; and we questioned witnesses on whether Dr Byron's proposed hybrid system for video game classification would be any clearer than the current system, given that there would still be two different logos for certain games—a BBFC rating on the front and a PEGI rating on the back. The Rt Hon Margaret Hodge MP, Minister of State at the Department for Culture, Media and Sport, accepted that this was a "perfectly legitimate concern, which is why we are going to have a period of consultation": she added that "a system which parents can easily understand is the most important objective that we must bear in mind and we will just have to test it".[353] Ofcom took a very similar view, arguing that the critical test is whether people understand and trust ratings.[354]

The relative strengths of the PEGI and the BBFC systems

198. No-one appeared to believe that the proposed hybrid system was a perfect solution. Witnesses representing the games industry generally favoured the PEGI system and they set out its strengths. Mr Darby, Operations Manager of the Video Standards Council, said that "the hybrid system would not have been a road that we would have suggested going down in the first place and … we would have preferred a single system. However, if the hybrid system is the one that is recommended PEGI will certainly work towards achieving that."[355] Paul Jackson, Director General of the Entertainment and Leisure Software Publishers Association (ELSPA), argued that only a self-regulatory system would be able to keep up with the expected dramatic increase in the number of games and games components (such as new features added to existing games), reaching possibly "100,000 game elements" in five years' time.[356] He questioned whether the BBFC would have the necessary resources and pointed out that PEGI was a "scaleable resource": the number of games publishers/developers would always equal the number of regulators.[357]

199. Microsoft pointed out that the PEGI system is more informative than the BBFC age classification, in that it gives parents both an age rating and a content rating for a game. Both Microsoft and ELSPA observed that PEGI was a self-regulatory system which was applied consistently across Europe.[358] Mr Ramsdale, Vice-President of EA Games, a games publisher, told us that "from our perspective, a multinational European system makes life a lot easier for a multinational publisher and retailer,"[359] and we can see the benefits and the convenience for the industry of a single assessment for authority to distribute a game across Europe. We note, however, that film distributors may face a similar obstacle but

[352] Q 581. See also Byron Review Action Plan, page 20

[353] Q 587

[354] Q 531

[355] Q 543

[356] Q 462

[357] Q 465

[358] Ev 35 and Q 85

[359] Q 464

nonetheless accept the requirement for individual assessment for distribution in each country .

200. Mr Jackson, Director General of ELSPA, proposed that the controls on supply under the Video Recordings Act 1984 should be afforded to the PEGI system in the UK: "We would then have one legal system that went from the shelf through to online and there would be the clearest possible world within which consumers could operate."[360] Mr Ramsdale described the ESRB (Entertainment Software Rating Board) system in the US, which imposes fines and product recalls and suspends future rating services if publishers do not comply with the rules: "We should look at the US model. […] That is a self-regulatory system with teeth and it works".[361] We were told that the ESRB system had "become the norm" in the United States and that retailers would not sell games without ESRB classifications; nor would console manufacturers develop consoles which would accept games without ESRB classifications.[362]

201. Despite the industry's doubts, the BBFC classification system has significant benefits. BBFC classifications are already recognised in statute; and, significantly, the BBFC logos are already understood and recognised by consumers, including parents who may not be familiar with games content but who can relate the logos to classification of film content. The Entertainment Retailers Association argued that the BBFC system would require considerably less consumer education to make it effective for games and concluded that "whilst neither the BBFC system nor PEGI meet all our requirements, we believe the BBFC system requires less work than PEGI to meet consumer needs".[363] The evidence on the relative familiarity of BBFC and PEGI symbols is contradictory: research commissioned by the BBFC suggested that the public would prefer to buy games from a website if it was clear that it was part of a BBFC scheme,[364] but the games industry presented research commissioned through YouGov, suggesting that the public did not perceive one system as being preferable to the other.[365]

202. The Government maintains that the BBFC method of classification is more thorough and rigorous than PEGI and believes that it "commands greater confidence".[366] The BBFC is confident that it would be able to absorb the extra work produced by the proposed new system: "We are certainly clear that it is a workable package and we do not have any difficulty at all with the resource implications."[367]

203. **We recognise the concerns that the hybrid system for games classification proposed by Dr Byron may not command confidence in the games industry and would not provide significantly greater clarity for consumers. We believe that, ideally, a single classification system should be adopted. While either of the systems operated by the**

[360] Q 464

[361] Q 466

[362] Information supplied to the Committee in the US by EA Games

[363] Ev 400

[364] Ev 315

[365] Ev 400

[366] Q 582

[367] Q 543

BBFC and by PEGI would be workable in principle, we believe that the widespread recognition of the BBFC's classification categories in the UK and their statutory backing offer significant advantages which the PEGI system lacks. We therefore agree that the BBFC should continue to rate games with adult content and should have responsibility for rating games with content appropriate only for players aged 12 or above, and that these ratings should appear prominently. Online distributors should be encouraged to take advantage of the BBFC.online scheme which should be promoted as offering greater confidence to parents about the nature of the game. While we hope that PEGI will work with the BBFC to develop a single system, distributors are of course free to continue to use PEGI ratings in addition, as they do at present.

Conclusions and recommendations

1. We agree that any approach to the protection of children from online dangers should be based on the probability of risk. We believe that incontrovertible evidence of harm is not necessarily required in order to justify a restriction of access to certain types of content in any medium. (Paragraph 53)

2. It is sensible that parents set boundaries for their children's online activities, but a totally risk-averse culture in parenting will not equip children to face dangers which they will inevitably encounter as they grow older. (Paragraph 54)

3. The Home Office Task Force on Child Internet Safety has, by common consent, done good work and has served its purpose well; but its loose funding and support structures have given the impression that its work is of a comparatively low priority. We agree with Dr Byron that the structure and funding of the Task Force should be formalised. We also welcome the announcement by the Government that the date for establishment of the Council is to be brought forward from April 2009 to September 2008. However, we are concerned at reports from some key players that there has been no contact with Government to take this forward and from others that there has been little opportunity to influence decisions as to how the Council will operate in practice. We expect the Government to address these issues urgently. (Paragraph 62)

4. We agree that the Council, at least in its early years, should be chaired by a Minister, to ensure that Council members have direct access to public policy-making. However, we question the proposed joint chairing arrangement, which excludes DCMS Ministers. We believe that it would be unfortunate if DCMS were to appear subsidiary in Council governance, given its role in media regulation, although we recognise the practical difficulties in sharing the chairing role between many Departments: indeed, we question whether co-chairing is desirable in principle. We invite the Government to consider carefully whether to appoint a single lead minister, either from one of the Departments represented or perhaps from the Cabinet Office. There may be a case in future for the Council to be chaired by someone who sits outside Government, particularly if the role of the Council is to expand. Given that the Government has accepted Dr Byron's recommendations in full, we believe it should now move quickly to provide a budget. (Paragraph 66)

5. While there might be an expectation that most of the Council's effort would be directed towards child protection, we believe that there is a danger of overlooking possible harm to vulnerable adults, and we recommend that the Government should give this proper consideration when deciding the Council's terms of reference. (Paragraph 67)

6. We are much impressed by the work of the Child Exploitation and Online Protection Centre and its close co-operation with charities such as the National Society for the Prevention of Cruelty to Children. However, we are concerned that levels of funding are not keeping pace with the increasing volume of work which is referred to the Centre, and we therefore encourage the Government to look

favourably on any request by CEOP for increased resources. We also welcome the financial contribution made by charities and industry, and we believe that the latter should be increased: business models for Internet-based services rely upon public confidence that networking sites are safe to use, and CEOP plays a large part in delivering that safety. (Paragraph 70)

7. We strongly recommend that terms and conditions which guide consumers on the types of content which are acceptable on a site should be prominent. It should be made more difficult for users to avoid seeing and reading the conditions of use: as a consequence, it would become more difficult for users to claim ignorance of terms and conditions if they upload inappropriate content. The UK Council for Child Internet Safety should examine this at an early stage and produce recommendations as to how it is best achieved. (Paragraph 85)

8. We are also concerned that user-generated video content on sites such as YouTube does not carry any age classification, nor is there a watershed before which it cannot be viewed. We welcome efforts by YouTube to identify material only suitable for adults, such as that containing foul language, and to develop potential controls to prevent children from accessing it. (Paragraph 86)

9. We do not believe that it is in the public interest for Internet service providers or networking sites to neglect screening content because of a fear that they will become liable under the terms of the EC E-Commerce Directive for material which is illegal but which is not identified. It would be perverse if the law were to make such sites more vulnerable for trying to offer protection to consumers. We recommend that Ofcom or the Government should set out their interpretation of when the E-Commerce Directive will place upon Internet service providers liability for content which they host or to which they enable access. Ultimately, the Government should be prepared to seek amendment to the Directive if it is preventing ISPs and websites from exercising more rigorous controls over content. (Paragraph 95)

10. We found the arguments put forward by Google/You Tube against their staff undertaking any kind of proactive screening to be unconvincing. To plead that the volume of traffic prevents screening of content is clearly not correct: indeed, major providers such as MySpace have not been deterred from reviewing material posted on their sites. Even if review of every bit of content is not practical, that is not an argument to undertake none at all. We recommend that proactive review of content should be standard practice for sites hosting user-generated content, and we look to the UK Council proposed by Dr Byron to give a high priority to reconciling the conflicting claims about the practicality and effectiveness of using staff and technological tools to screen and take down material. (Paragraph 96)

11. File titles and screening tools can help to identify files which appear to present a particular risk of exposure to inappropriate material. We encourage sites which handle user-generated content to develop as a priority technological tools to screen file titles and prevent the upload of—or quarantine—material which potentially violates terms and conditions of use until it has been reviewed by staff. We also encourage sites to share their knowledge and expertise at the UK Council on Child

Internet Safety, with a view to developing codes of practice for prior screening of material. (Paragraph 97)

12. We find it shocking that a take-down time of 24 hours for removal of child abuse content should be an industry standard. (Paragraph 98)

13. We believe that there is a need for agreed minimum standards across industry on take-down times in order to increase consumer confidence. We recommend that the UK Council on Child Internet Safety should work with Internet-based industries to develop a consistent and transparent policy on take-down procedures with clear maximum times within which inappropriate material will be removed. This should be subject to independent verification and publication. (Paragraph 99)

14. We await the announcement by the Ministry of Justice on whether the law might be strengthened to help prevent the use of the Internet to encourage suicide. Even if it concludes that the offence of assisting suicide is clear enough in law to enable successful prosecutions of those responsible for websites which assist or encourage suicide, we believe that the law should not be the only means of controlling access. The characteristics of the offence should be clear enough in law to enable access to such sites to be blocked on a voluntary basis, possibly through the procedures established by the Internet Watch Foundation. The UK Council for Child Internet Safety should accord a high priority in its work programme to discussions with the Ministry of Justice on whether the law on assisted suicide is worded clearly enough to include websites which encourage suicide and to enable action to be taken to block access to websites which assist or encourage suicide. (Paragraph 117)

15. At a time of rapid technological change, it is difficult to judge whether blocking access to Internet content at network level by Internet service providers is likely to become ineffective in the near future. However, this is not a reason for not doing so while it is still effective for the overwhelming majority of users. (Paragraph 119)

16. We believe that there would be advantage in establishing a forum at which governments or regulators from across the world could try to find common ground on how access to content on the Internet should be treated. This may, in time, lead to a more co-ordinated effort in frustrating access to material which is widely perceived as harmful. We recommend that the Government should take a lead in establishing such a forum. (Paragraph 124)

17. It is clear that many users of social networking sites, particularly children, do not realise that by posting information about themselves, they may be making it publicly available for all to see. We recommend that social networking sites should have a default setting restricting access and that users should be required to take a deliberate decision to make their personal information more widely available. We also recommend that consideration be given to alerting users through pop-up displays about the risks involved in submitting personal details without restricting access. (Paragraph 128)

18. We commend Microsoft for providing a facility for direct reporting to the Child Exploitation and Online Protection Centre within Windows Live Messenger. We believe that high profile one-click facilities for reporting directly to law enforcement

and support organisations are an essential feature of a safe networking site. We recommend that the UK Council for Child Internet Safety should impress upon providers of networking services the value of direct one-click reporting from their websites to law enforcement agencies and voluntary sector organisations with expertise in offering support to vulnerable people. We also believe that facilities for reporting abuse should be obvious to users and should be directly accessible from all relevant pages of a website, close to the entry point. We would expect providers of all Internet services based upon user participation to move towards these standards without delay. (Paragraph 132)

19. We recommend that network operators and manufacturers of mobile devices should assess whether it is technically possible to enable images sent from mobile devices to be traced and viewed by law enforcement officers with the appropriate authority. (Paragraph 138)

20. We commend Microsoft for their efforts to ensure that there are varied and effective parental controls built in to their hardware. We believe that other console manufacturers should be encouraged at least to match these. We hope that this matter will also be considered at an early date by the UK Council on Child Internet Safety. (Paragraph 140)

21. We expect the Government to apply continuing, and if necessary, escalating pressure on Internet service providers who are showing reluctance to block access to illegal content hosted abroad. In a lucrative market, the cost to Internet service providers of installing software to block access to child pornography sites should not come second to child safety. (Paragraph 146)

22. We believe that leaving individual companies in the Internet services sector to regulate themselves in the protection of users from potential harm has resulted in a piecemeal approach which we find unsatisfactory. Different practices are being followed and there is a lack of consistency and transparency, leading to confusion among users. Nor is there any external mechanism for complaints about services provided by Internet-based industries to be considered by an independent body. However, we do not believe that statutory regulation should be the first resort. Instead, we propose a tighter form of self-regulation, applied across the industry and led by the industry. We therefore call on the industry to establish a self-regulatory body which would agree minimum standards based upon the recommendations of the UK Council for Child Internet Safety, monitor their effectiveness, publish performance statistics and adjudicate on complaints. (Paragraph 153)

23. We recognise that a number of companies may choose to set higher standards for their own commercial reasons, but the public need the assurance that certain basic standards will be met. This is particularly important in the area of child protection and Internet safety. However, the new body might also take on the task of setting rules governing practice in other areas such as on-line piracy and peer to peer file-sharing, and behavioural advertising, which although outside the scope of this inquiry are also of public concern. Given the global nature of the industry, it is impossible to make membership compulsory for all service providers, but a widespread publicity campaign should ensure that consumers are aware that they

can have confidence in the standards of protection and reputable practice which membership of the body carries with it and that this cannot be guaranteed by those companies that choose not to join. (Paragraph 154)

24. Our preferred model for any new body to maintain standards among providers of Internet-based services is that of the Advertising Standards Authority, which is generally successful at securing compliance with codes for advertising standards but which, if necessary, may refer companies which persistently breach those standards to statutory regulators that can apply penalties. (Paragraph 155)

25. We commend the Government for the action it has taken to motivate the Internet industry, the voluntary sector and others to work together to improve the level of protection from risks from the Internet, particularly for children. However, we regret that much of this work remains unknown and has therefore done little to increase public confidence. We look to the UK Council to build on the existing agreements and to ensure a much greater public awareness of what has already been achieved. (Paragraph 157)

26. We also note that the Government originally suggested that four different Ministers should give evidence to our inquiry and it does seem that there is scope for improved co-ordination of activity between different Government departments. We recommend that a single Minister should have responsibility for co-ordinating the Government's effort in improving levels of protection from harm from the Internet, overseeing complementary initiatives led by different Government departments, and monitoring the resourcing of relevant Government-funded bodies. (Paragraph 159)

27. We endorse the thrust of Dr Byron's recommendations on improving media literacy, and we commend her for her approach. However, we believe that the one-stop shop will only be worth locating on the DirectGov website if search tools, social networking sites, video-sharing sites and Internet service providers offer a direct link: otherwise the one-stop shop will languish in obscurity. We also recommend that all new computer equipment sold for home use should be supplied with a standard information leaflet, to be agreed with the IT hardware and software industries through the UK Council on Child Internet Safety, containing advice for parents on Internet safety tools and practices. (Paragraph 185)

28. We agree with Ofcom that parents will need to take on greater responsibility for protecting children from harm from the Internet and from video games. In particular, they should be aware of the consequences of buying devices which allow unsupervised access to the Internet; they should have more knowledge of young children's social networking activities and be more familiar with video game content, thereby gaining a better understanding of the risks; and they should, wherever possible, discuss those risks openly with their children. We recommend that the UK Council for Child Internet Safety should investigate ways of communicating these messages to parents. (Paragraph 186)

29. We recognise the concerns that the hybrid system for games classification proposed by Dr Byron may not command confidence in the games industry and would not provide significantly greater clarity for consumers. We believe that, ideally, a single

classification system should be adopted. While either of the systems operated by the BBFC and by PEGI would be workable in principle, we believe that the widespread recognition of the BBFC's classification categories in the UK and their statutory backing offer significant advantages which the PEGI system lacks. We therefore agree that the BBFC should continue to rate games with adult content and should have responsibility for rating games with content appropriate only for players aged 12 or above, and that these ratings should appear prominently. Online distributors should be encouraged to take advantage of the BBFC.online scheme which should be promoted as offering greater confidence to parents about the nature of the game. While we hope that PEGI will work with the BBFC to develop a single system, distributors are of course free to continue to use PEGI ratings in addition, as they do at present. (Paragraph 203)

Formal Minutes

Tuesday 22 July 2008

Members present:

Mr John Whittingdale, in the Chair

Philip Davies	Alan Keen
Paul Farrelly	Helen Southworth

Draft Report (Harmful Content on the Internet and in Video Games), proposed by the Chairman, brought up and read.

Ordered, That the Chairman's draft Report be read a second time, paragraph by paragraph.

Paragraphs 1 to 203 read and agreed to.

Summary agreed to.

Resolved, That the Report be the Tenth Report of the Committee to the House.

Ordered, That the Chairman make the Report to the House.

Ordered, That embargoed copies of the Report be made available, in accordance with the provisions of Standing Order No. 134.

Written evidence was ordered to be reported to the House for printing with the Report.

Written evidence was ordered to be reported to the House for placing in the Library and Parliamentary Archives.

[Adjourned till Tuesday 7 October at 10.15 am

Witnesses

Tuesday 26 February 2008

Tuesday 4 March 2008

Tuesday 18 March 2008

Tuesday 1 April 2008

Tuesday 29 April 2008

Tuesday 13 May 2008

Wednesday 14 May 2008

List of written evidence

List of unprinted evidence

The following memoranda have been reported to the House, but to save printing costs they have not been printed and copies have been placed in the House of Commons Library, where they may be inspected by Members. Other copies are in the Parliamentary Archives, and are available to the public for inspection. Requests for inspection should be addressed to The Parliamentary Archives, Houses of Parliament, London SW1A 0PW (tel. 020 7219 3074). Opening hours are from 9.30 am to 5.00 pm on Mondays to Fridays.

Orange UK
Sexual Freedom Coalition
Child Exploitation and Online Protection Centre
Cyber-Rights.org
Advertising Association
Mobile Broadband Group
London Internet Exchange
European Commission
Mediamarch
PAPYRUS
Media Literary Task Force
Broadband Stakeholder Group
ELSPA
Department for Children, Schools and Families and the Home Office
Electronic Arts (EA Games)
Andrew Tinton
Games Up?
Ofcom
Fox Interactive Media

List of Reports from the Committee during the current Parliament

Session 2005–06

First Special Report	Maritime Heritage and Historic Ships: Replies to the Committee's Fourth Report of Session 2004-05	HC 358
First Report	Broadcasting Rights for Cricket	HC 720
Second Report	Analogue Switch-off	HC 650 I, II
Third Report	Preserving and Protecting our Heritage	HC 912 I, II, III
Fourth Report	Women's Football	HC 1357
Second Special Report	Women's Football: Replies to the Committee's Fourth Report of Session 2005–06	HC 1646

Session 2006–07

First Report	Work of the Committee in 2006	HC 234
Second Report	London 2012 Olympic Games and Paralympic Games: funding and legacy	HC 69 I, II
Third Report	Call TV quiz shows	HC 72
Fourth Report	Call TV quiz shows: Joint response from Ofcom and ICSTIS to the Committee's Third Report of Session 2006-07	HC 428
Fifth Report	New Media and the creative industries	HC 509 I, II
Sixth Report	Caring for our collections	HC 176 I, II
Seventh Report	Self-regulation of the press	HC 375
First Special Report	Self-regulation of the press: Replies to the Committee's Seventh Report of Session 2006–07	HC 1041

Session 2007–08

First Report	Public service content	HC 36 I, II
First Special Report	Public service content: Response from Ofcom to the Committee's First Report of Session 2007–08	HC 275
Second Report	Ticket touting	HC 202
Third Report	Work of the Committee in 2007	HC 234
Fourth Report	BBC Annual Report and Accounts 2006–07	HC 235
Fifth Report	On-course horserace betting	HC 37
Second Special Report	On course horserace betting: Government Response to the Committee's Fifth Report 2007–08	HC 549
Sixth Report	London 2012 Games: the next lap	HC 104 I, II
Seventh Report	European Commission White Paper on Sport	HC 347
Third Special Report	European Commission White Paper on Sport: Government Response to the Committee's Seventh Report 2007–08	HC
Eighth Report	Tourism	HC 133 I, II
Ninth Report	Draft Cultural Property (Armed Conflicts) Bill	HC 693