



House of Commons
Culture, Media and Sport
Committee

Online safety

Sixth Report of Session 2013–14

Volume II

Additional written evidence

*Ordered by the House of Commons
to be published [date]*

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*) (Chair)
Mr Ben Bradshaw MP (*Labour, Exeter*)
Angie Bray MP (*Conservative, Ealing Central and Acton*)
Conor Burns MP (*Conservative, Bournemouth West*)
Tracey Crouch MP (*Conservative, Chatham and Aylesford*)
Philip Davies MP (*Conservative, Shipley*)
Paul Farrelly MP (*Labour, Newcastle-under-Lyme*)
Mr John Leech MP (*Liberal Democrat, Manchester, Withington*)
Steve Rotherham MP (*Labour, Liverpool, Walton*)
Jim Sheridan MP (*Labour, Paisley and Renfrewshire North*)
Mr Gerry Sutcliffe MP (*Labour, Bradford South*)

The following members were also a member of the committee during the parliament:

David Cairns MP (*Labour, Inverclyde*)
Dr Thérèse Coffey MP (*Conservative, Suffolk Coastal*)
Damian Collins MP (*Conservative, Folkestone and Hythe*)
Alan Keen MP (*Labour Co-operative, Feltham and Heston*)
Louise Mensch MP (*Conservative, Corby*)
Mr Adrian Sanders MP (*Liberal Democrat, Torbay*)
Mr Tom Watson MP (*Labour, West Bromwich East*)

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.

Publication

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 www.parliament.uk/cmscom. A list of Reports of the Committee in the present Parliament is at the back of this volume.

The Reports of the Committee, the formal minutes relating to that report, oral evidence taken and some of the written evidence are available in a printed volume.

Additional written evidence is published on the internet only.

Committee staff

The current staff of the Committee are Elizabeth Flood (Clerk), Grahame Danby (Second Clerk), Kevin Candy (Inquiry Manager), Emily Gregory (Senior Committee Assistant), Keely Bishop (Committee Assistant) and Jessica Bridges-Palmer (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; the Committee's email address is cmscom@parliament.uk

List of additional written evidence

(published in Volume II on the Committee's website www.parliament.uk/cmscom)

| | <i>Page</i> |
|---|---------------|
| 1 Dr Peter Dawe OBE | Ev w1 |
| 2 Dr Claire Hardaker | Ev w2 ; Ev w7 |
| 3 Remote Gambling Association | Ev w7 |
| 4 Ann Farmer | Ev w10 |
| 5 Kirsty Hopley | Ev w10 |
| 6 Dr Peter Nelson | Ev w11 |
| 7 British Board of Film Classification (BBFC) | Ev w13 |
| 8 Arqiva | Ev w18 |
| 9 James Griffiths | Ev w22 |
| 10 Christopher G. H. Thomas | Ev w22 |
| 11 John Edgar Cameron Lowe | Ev w23 |
| 12 Norfolk Library and Information Service | Ev w23 |
| 13 Phil Alexander | Ev w25 |
| 14 Ben Hardwick | Ev w25 |
| 15 John R Edwards | Ev w26 |
| 16 Chris Evershed | Ev w27 |
| 17 EE Limited | Ev w28 |
| 18 BCS The Chartered Institute for IT | Ev w32 |
| 19 Dudley Friend Clayson | Ev w36 |
| 20 PAPYRUS Prevention of Young Suicide | Ev w37 |
| 21 EU Kids Online | Ev w38 |
| 22 Rolf Smith | Ev w43 |
| 23 Mediawatch-UK | Ev w45 |
| 24 South West Grid for Learning | Ev w47 |
| 25 British Sky Broadcasting Limited ('Sky') | Ev w51 |
| 26 Big Brother Watch | Ev w53 |
| 27 BT | Ev w56 |
| 28 Russell Hopwood | Ev w59 |
| 29 Stuart Taylor | Ev w60 |
| 30 Richard Browning | Ev w61 |
| 31 Timothy Michael Johnston | Ev w62 |
| 32 Lloyd Johnston | Ev w62 |
| 33 John Carruth | Ev w63 |
| 34 Rob Barry | Ev w64 |
| 35 Barry Saltmarsh | Ev w65 |
| 36 Safermedia | Ev w66 |
| 37 John Reiner | Ev w69 |
| 38 Family Online Safety Institute | Ev w69 |
| 39 Terry James | Ev w72 |
| 40 Film Distributors' Association | Ev w73 |

| | | |
|----|--|---------|
| 41 | Information Commissioner's Office | Ev w74 |
| 42 | Virgin Media | Ev w77 |
| 43 | The Police Federation of England and Wales | Ev w84 |
| 44 | End Violence Against Women Coalition | Ev w85 |
| 45 | Childnet International | Ev w88 |
| 46 | Ukie | Ev w92 |
| 47 | The Children's Society | Ev w96 |
| 48 | Eric and Esme Bricknell | Ev w97 |
| 49 | Stonewall | Ev w98 |
| 50 | FPA and Brook | Ev w100 |
| 51 | Michael J Smaldon | Ev w109 |
| 52 | Prof Andy Phippen | Ev w110 |
| 53 | Ahmadiyya Muslim Community UK | Ev w113 |
| 54 | Sex Education Forum | Ev w117 |
| 55 | Net Children Go Mobile | Ev w119 |
| 56 | British Naturism | Ev w120 |
| 57 | Open Rights Group | Ev w122 |
| 58 | Russell Pillar | Ev w126 |
| 59 | CARE (Christian Action Research and Education) | Ev w127 |
| 60 | Malcolm Holmes | Ev w130 |
| 61 | Microsoft UK | Ev w131 |
| 62 | The Authority for Television on Demand | Ev w132 |
| 63 | Intellect | Ev w139 |
| 64 | Telefonica UK Ltd | Ev w142 |
| 65 | National Centre for Cyberstalking Research | Ev w143 |
| 66 | Ethos Capital Ltd | Ev w145 |

Written evidence

Written evidence submitted by Dr Peter Dawe OBE

1. THE FLAVOURED INTERNET FOUNDATION

Internet damage limitation. Dr. P Dawe OBE, Founder Internet Watch Foundation, 2013.

2. INTRODUCTION

Once again there is a public furore about Internet content. However, this time the debate is messy and ill-disciplined, as many voices are speaking about many issues: Child protection, legality of content, censorship, financial predation, bullying to name just a few.

Policy makers are in an impossible position! Caught between protection and censorship with the added problems due to the global nature of the Internet.

3. This paper outlines a means of mitigating the problems based on the genesis of The Internet Watch Foundation by the person who lead the founding of IWF.

4. A SOLUTION

It is our view that the problem is not a legislative problem, but a market problem. Previously, there has been a diversity of media channels with each channel being moderated by an “editor”.

The Internet needs to offer the public a choice of “flavours” of Internet, similar to how people choose their newspaper, TV channel or indeed their preferred supermarket.

5. WHY IS THERE MARKET FAILURE IN SELECTIVE INTERNET?

- Currently providing a moderated view (Fenced Garden) of the Internet isn’t economically viable.
- The Internet is so large as to be difficult, nay impossible, to comprehensively categorise all content.
- The choice of “flavour” is also difficult as each person has their own set of prejudices, in many dimensions. Eg Extent of naked flesh, Violence, Religion.
- Service providers are, understandably, reluctant to be seen as the arbiters of taste and legality.
- The threat of a defamation action when a content provider is censored on the basis of an algorithm, particularly if the censorship is due to “business morality”.
- Computer applications to implement filtering have been proprietary and not comprehensive in their use of available tools.
- Multiple legislative jurisdictions have to be considered.

6. Several attempts have been made to provide the public with filtered content, however typically these are from a singular view-point (eg Western liberal Christian tradition), which means the cost of creating the filter list has to be spread over a small user base.

7. CREATING A VIABLE MARKETPLACE

- There is a need for an open architecture for classification.
- The problem is too big for a individual players.
- Web authors do not want to negotiate with individual classification services and editors.
- New applications can be implemented using existing infra-structure.
- Editors want to be able to choose their own filtering thresholds and classes.

8. TACTICAL IMPLEMENTATION STEPS

- Political encouragement to entrepreneurs to implement diverse Internet “flavoured” services.
- Extension of the legal protection, enjoyed by newspaper editors against civil claims from content owners, to filtering services.
- A legal requirement on Internet service providers to be network neutral in regard to providers of Flavoured Internet.
- The implementation of a series of demonstration technologies and services.

9. LEADERSHIP NOT COMMITTEE

The genesis of Internet Watch Foundation should be seen as a model for deployment. Internet Watch was founded, NOT BY CONSENSUS, but designed and implemented through the maverick leadership of Mr Peter Dawe. The players (Service providers, Government, Police, Politicians and the Press) are individually impotent.

Each has conflicting objectives, all consider the other players as responsible, irresponsible, ignorant, idealistic, imposing impossible costs, ducking their responsibility etc.

10. However, with a more sophisticated set of players, it is less likely that a maverick leader will not be able to overcome the likely barriers alone. Political endorsement of this initiative, for a finite period (two years), would encourage many of the other players to also support the initiative. Thus allowing the model design to be finalised, proof of concept completed and for the model to be promoted to all players world-wide.

11. Note: Other initiatives, such as consensus building committees, can still be undertaken in parallel with this proposal.

12. FUNDING

For an effective team to complete the design, prove concept and importantly to sell the model internationally, we estimate that a budget over the two years of £500,000 would suffice. A requirement of the design is that it is ultimately self-funding in operation. (Internet Watch cost under £50,000 to set up, and was completed in less than 12 months, a voluntary levy on the industry has funded it since.)

13. The Dawe Charitable Trust believe it can catalyse the actions needed for this global initiative, recruiting support from the industry, government, religious, freedom-of-speech and other groups.

14. Dawe Charitable Trust already has an experienced core team committed to working on the initiative.

15. The Dawe Charitable Trust is seed-funding this initiative (£50,000), and the team will seek to design and implement a model regardless. However adoption of the above recommendation will both speed the initiative and improve the likelihood of global success.

September 2013

Written evidence submitted by Dr Claire Hardaker

SUMMARY

In this document I discuss the following four points:

- What facilitates abusive or threatening online comments (ie what makes it “easy”?)
- What motivates abusive or threatening online comments (ie what makes people do it?)
- Measures **unlikely** to reduce abusive or threatening online comments (ie what won’t stop it?)
- Measures likely to reduce abusive or threatening online comments (ie what could stop it?)

PRELIMINARY COMMENTS

(1) Whilst my research has covered strategies of content filtering, it relates better to the discussion of “preventing abusive or threatening comments”, and less directly to “protecting minors from adult content” or “filtering extremist material such as child abuse imagery”. I therefore do not comment on these two areas.

(2) A crucial point note, however, is that *filtering* content intended to promote harmful behaviour (eg terrorism, violence) is unlikely to deal with the online grooming responsible for inciting these behaviours. Grooming is typically an interactive process involving a manipulator persuading a vulnerable target to undertake action that is in the manipulator’s interest, and typically harmful to the target (eg extremist violence, suicide, self-harm, age-inappropriate sexual behaviour, etc.).

(3) Such grooming is likely to occur in interactive environments such as chatrooms, messageboards, and via private direct-message software (eg Windows Live Messenger) where content filtering will struggle to apply, and where processes of moderation are likely to be far more effective. I would therefore suggest that content filtering as a strategy for dealing with material intended to promote terrorism or other acts of violence is unlikely to tackle this point with much success.

What facilitates abusive or threatening comments online?

(4) There are arguably three major factors (though easily more besides):

ANONYMITY

(5) The internet offers a perceived anonymity that has no real parallel offline, and this appearance of invisibility encourages the user to feel that they can do unpleasant things with a highly reduced risk of suffering any consequences. In turn, the sense of being invulnerable encourages disinhibition: the user thinks that she is safe from repercussions, so behaves in a mildly objectionable way. Each time there is no negative consequence, her behaviour may gradually escalate.

(6) By itself, however, anonymity does not explain why the internet seems to bring the worst out in some, since many of us are online and anonymous all the time, yet would never think to behave in this way. A second issue to consider, then, is detachment.

DETACHMENT

(7) Linked to disinhibition is the way that the internet allows us to shut down our empathy, and in particular, our compassion. In fact, we can choose not to empathise at will, especially when dealing with someone we dislike. The internet, however, drastically increases this ability, and allows us to emotionally distance ourselves—not just from people we don't like but also from those we don't even know—in several ways:

- (a) *Dehumanising*: Because we lose many indications of emotional response (eye contact, tone of voice, facial expressions) it is easier to “forget” that we are communicating with another human. Instead, we have only the words and/or images sent back and forth.
- (b) *Devaluing*: The above means that we can downplay any emotional reaction. If they claim to be offended or hurt, because we don't see that reaction, it is easier to believe that they are lying or exaggerating. It is also easier to quickly forget the incident, whilst it may linger in the other's mind for days.
- (c) *Victim-blaming*: It can be easier for the bully/troll to shift the responsibility for what they are doing from themselves, and blame their victim for what is happening, because, eg, they're famous, or they made a tribute page public, etc. This stance is typically also indicated by “solutions” such as telling the victim that if they don't like it, they should “get off the internet”.
- (d) *Self-vindicating*: It can also be easier to diminish the severity of our behaviour to ourselves. Because we each inhabit our own heads, it seems obvious to us just how seriously we meant something, so when trolls/cyberbullies are confronted, we tend to hear excuses like, “Stuff said on the internet isn't real. I was just joking. I obviously didn't really mean that [rape-threat/defamatory statement/etc].” Our innate bias means that we are more likely to adopt such a self-supporting viewpoint than to judge our own behaviour as reprehensible.

ENTERTAINMENT

(8) The third aspect that seems to encourage some to be deliberately mean online long predates the internet. It is simply the human tendency to enjoy and glorify aggression. Evidence for this can be found worldwide, stretching back over millennia. For brevity, however, we need only look at ancient military artefacts (eg the Bayeux tapestry, Homer's *Iliad*, *Beowulf*), the sports descended directly from warfare (javelin, archery, fencing, boxing, wrestling, martial arts), and archaeology built especially for the enjoyment of bloodshed (eg the Coliseum, the Hippodrome).

(9) Today, one glance at mainstream entertainment demonstrates that this interest is not remotely abated. For instance, *The Hunger Games* is a book series about individuals forced to fight to the death for a reality television show. *Shawshank Redemption* tells of a man wrongly convicted for the murder of his wife and incarcerated in a brutal, corrupt prison where inmates are beaten to death, shot, and raped. *The X Factor* television series places competitors into highly stressful, even cruel environments with antagonistic judges. And many of the biggest games titles, such as the *Call of Duty*, *Halo*, and *Grand Theft Auto* series, involve players simulating extreme violence and murder.

(10) The above should demonstrate that humans are entertained by violence, and that this is by no means a new phenomenon brought about by digital media. For some, however, simply consuming aggression-based entertainment from fiction (eg books, films) or simulation (eg games, sports) is not enough. For them, the internet presents a virtual Coliseum where they can amuse themselves by attacking others without risk of “injury”, since they can hide behind a cloak of anonymity, and silence their own conscience by ignoring their target's feelings.

What motivates abusive or threatening comments online?

(11) To reiterate a point from above, whilst many of us are frequently online anonymously *and* enjoy consuming violence (it is a rare person who hasn't watched an action movie!), it is still a relatively small number who feel motivated to take advantage of the conditions that the internet presents, and to actually engage in abusive or threatening online behaviour. In the same way, many of us drive, but however annoyed we may become behind the wheel, mercifully few of us ever turn our car into a lethal weapon.

(12) In other words, each individual needs a trigger, or motive to push them into using the internet as a weapon. Unsurprisingly, the evidence suggests that there is no single, over-riding motive for being abusive or threatening online, but that whilst there certainly are trends, there are also many unique cases. Some of those broad trends include:

- (a) *Boredom, a need for entertainment*: This is perhaps the most trivial reason (and therefore, perhaps also the most frustrating and difficult to resolve)—simply too much free time after school, at work, or between jobs. These are the individuals who are killing time, and even seeking impress others of a similar mindset. Groups of trolls coalesce on sites like 4chan, post

links to targets that might prove “fun”, and compete against each other to see who can be the funniest, cleverest, or most extreme. They may also organise troll raids via more secure systems (eg *IRC*, *Torchat*), and train newer recruits in how to be less identifiable online, eg by sharing information about identity-protecting software such as *TOR*, *I2P*, and *Psiphon*.

- (b) *A need for attention*: these individuals seem to display a craving for any kind of attention, whether positive or negative. Such individuals may also post annoyingly implausible stories, grand claims, age-inappropriate content, etc. This may be symptomatic of emotional, social, and/or psychological problems.
- (c) *Revenge, disenfranchisement*: these appear to be individuals who feel cheated, short-changed, or otherwise wronged on a personal level, and appear to want to “fix” this by making the object of their malice feel as miserable as themselves. This may be symptomatic of a struggling economy, eg the student who can’t find work and has therefore taken to targeting his local MP.
- (d) *Politics, activism*: whilst the motive in its own right may be good (eg fighting for racial equality) the method may not meet that same moral standard. This said, it’s easier to comprehend why individuals might choose this noisy, attention-grabbing route if we consider that letters to politicians, newspapers, and economists are all too easily ignored. This may be symptomatic, therefore, of a political system that appears (to the trolls/bullies) to ignore their voices.

(13) In summary, motivations for posting abusive/threatening content can spring from a number, and a mixture of sources, including emotional, psychological, social, political, economical, etc. This means that there is likely to be no *single* approach that will have any meaningful impact on this issue. Instead, it is far more likely to require addressing on multiple fronts. I discuss this area next.

Measures unlikely to reduce online abuse or threats

(14) There are two classic “solutions” that have been proposed to fix online abusive comments. I deal with them briefly since they merit very little serious consideration.

REMOVE ANONYMITY

(15) In a nutshell, this is borderline impossible, if only because it is unenforceable, and unworkable. Even if all countries agree to legally mandating online identity disclosure (unlikely) the costs of setting up, administrating, and then enforcing it would be staggering. Further, we need only consider the risks inherent in having a child’s name, age, location, etc, available online to realise that online identity disclosure would actually create more dangers than anonymity currently averts.

STOP USING THE INTERNET (OR THE SITE IN QUESTION)

(16) This is not only bizarrely unrealistic, since the internet is now ubiquitous, it is also ineffective (kids don’t need a single device to be cyberbullied) and puts responsibility on the victim, rather than the attacker (see victim-blaming, para. (7(c)) above).

Measures likely to reduce online abuse or threats

(17) There is no single answer to this complex problem, but several smaller improvements can, collectively, advance online safety. I therefore recommend five ways forward.

EDUCATION, RESOURCES, AND TRAINING FOR CHILDREN AND YOUNG ADULTS

(18) In a perfect world, we would always choose prevention over cure, but this requires well-informed vigilance both from potential targets and from those responsible for protection. At present, Childnet does outstanding work, teaching school-children to be safe *and kind* online, and I welcome the fact that online safety has been introduced across the 2014 National Curriculum.

(19) For best effect, however, these lessons need to be appropriately supported (see paras. (21)–(23) below), sufficiently detailed/thorough, and adopted across *all* schools (private, public, and free). These lessons also should not be restricted purely to Computing, but should be adopted across a number of classes, including PSHEE and Citizenship.

(20) However, in order for this to be successful, teachers themselves need to be well-trained in the safety measures, in tell-tale signs, and in appropriate strategies of intervention. Teachers also need the support of parents and caregivers, and this leads into a second area of improvement.

EDUCATION, RESOURCES, AND TRAINING FOR PARENTS, CAREGIVERS, AND TEACHERS

(21) The assistance that Childnet currently offers teachers is also invaluable, but it could be substantially underpinned with compulsory online safety training in all PGCEs, since NSPCC research shows that far too

many teachers currently don't feel confident when it comes to advising pupils on safe social network practices.¹

(22) Meanwhile, parents would benefit from proactive, face-to-face training in:

- (a) signs indicative of cyberbullying (whether as victim or bully);
- (b) ways to keep children safe online² (technologically, behaviourally); and
- (c) the many organisations that offer help and advice (eg BeatBullying,³ Childline,⁴ Childnet,⁵ Get Safe Online,⁶ IWF,⁷ NSPCC,⁸ SIC,⁹ NHS,¹⁰ CEOP¹¹).

(23) Whilst these organisations all do invaluable work, they cannot be a standalone solution. A third area of improvement, then, is through sites themselves.

SITE TOOLS, RESPONSIBILITIES, AND PROCESSES

(24) We generally expect social networks to offer the tools and support to keep us safe. Indeed, the expectation seems fairly reasonable. If Mr Smith wants to profit from people buying his goods or services, his products and premises must meet the relevant legal requirements to protect customers from loss and harm. However, should Mr Smith want to profit from people using his social network, in the UK at least there appear to be no similar legal requirements.

(25) It seems reasonable to argue that the opportunity to profit from a social network should also entail a duty of care towards that site's users. However, whilst most social networks require registrants to enter into agreements forbidding abusive behaviour, beyond that, sites differ widely in the availability, sophistication, and transparency of their safety features. At the most basic level, social networks should:

- (a) allow users to control their own environment (eg privacy settings);
- (b) flag up content for the site to manage (eg report abuse buttons);
- (c) proactively use their own management tools (eg IP blocks); and
- (d) publish clear guidelines on how they will deal with complaints, handle abuse reports, and cooperate with criminal investigations.

(26) At present, whilst some sites offer all of these and more, others provide none, and some even appear to stonewall those trying to tackle online abuse.¹² This takes us into a fourth area of improvement—enforcement.

EDUCATION, RESOURCES, AND TRAINING FOR POLICE

(27) Where cases become too serious for a user or site to deal with, we would naturally turn to the police. However, whilst SOCA¹³ does tackle cybercrime, its focus tends to divide between child sexual exploitation and online fraud. SOCA and the Police Central e-Crime Unit¹⁴ are forming a new National Cybercrime Unit,¹⁵ but it remains unclear whether online abuse will form part of this organisation's remit.

(28) This means that for now at least, online abusive messages and threats are more likely to be dealt with by ordinary police officers, and that makes it difficult for the average non-high-profile individual to find appropriately trained police who will take their complaint seriously.¹⁶ In short, it is vital that we have the necessary resources and training for police, including:

- (a) *Perception change*: online offences are “real crimes” that should be taken seriously; users can't just resolve the problem by simply “switching off” (see para. (16) above).
- (b) *Basic training*: unsurprisingly, non-specialist officers appear to be largely unaware of the sheer scope of online “misbehaviours” that exist, how online attackers work, their strategies of concealment, standard denial excuses (eg “yes it came from my computer but I didn't send it”), methods of gathering evidence, the investigation that needs carrying out, etc. This is an issue that can only be resolved with extensive training. Without it, officers are likely to shy away from or find excuses for avoiding such areas, in turn institutionally embedding the concept that they only deal with “real” (ie offline) crime.

¹ www.nspcc.org.uk/Inform/resourcesforprofessionals/online-safety/statistics-online-safety_wda93975.html

² <http://consumers.ofcom.org.uk/2009/12/child-internet-safety-strategy-launched/>

³ www.beatbullying.org/

⁴ www.childline.org.uk/Explore/Bullying/Pages/online-bullying.aspx

⁵ www.childnet.com/

⁶ www.getsafeonline.org/

⁷ www.iwf.org.uk/

⁸ www.nspcc.org.uk/help-and-advice/for-parents/online-safety/online-safety_wdh99554.html

⁹ www.saferinternet.org.uk/advice-and-resources

¹⁰ www.nhs.uk/Livewell/Bullying/Pages/Cyberbullying.aspx

¹¹ www.thinkuknow.co.uk/

¹² www.theguardian.com/society/2013/aug/09/cyberbullying-mother-fight-askfm

¹³ www.nationalcrimeagency.gov.uk/

¹⁴ <http://content.met.police.uk/Site/pceu>

¹⁵ www.gov.uk/government/policies/keeping-the-uk-safe-in-cyberspace/supporting-pages/setting-up-a-national-cyber-crime-unit

¹⁶ www.theguardian.com/society/2013/aug/09/cyberbullying-mother-fight-askfm

- (c) *More resources*: even were the above not an issue, officers also appear to be largely under-resourced in terms of time. The solution to this seems to be an extension to the remit of CEOP, SOCA, or the newly-proposed NCU (see para. (27) above).

LEGISLATION AND GUIDANCE

(29) Assuming that a case is investigated by the police and the CPS decides to pursue criminal charges, many of the Acts that might be employed (eg Malicious Communications Act 1988, §5 of the Public Order Act 1986, Protection from Harassment Act 1997, Communications Act 2003) were created before the advent of major social networks, and so are imperfectly equipped to deal with the new behaviours that these sites have created.

(30) For instance, the most recent, relevant legislation, the Communications Act, came into force in July 2003. However, an Act of this magnitude—more than 250,000 words spanning over four hundred sections—takes years to write and enact. The section relevant to online behaviour (§127) is therefore far more heavily informed by the internet of the 1990s than that of the new millennium. Meanwhile, massive, ubiquitous social networks like *Facebook* and *Twitter* were founded 2004 and 2006 respectively. As sites like these have evolved, so too have the behaviours associated with them, yet the legislation remains largely unchanged.

(31) Whilst the CPS published guidelines¹⁷ on prosecuting cases involving communications sent via social media in June this year, like much current legislation designed for supposedly-similar offline behaviours, these guidelines do not explicitly address the critical differences that the online environment offers:

- (a) the speed with which content can be reproduced;
- (b) the breadth and sensitivity (eg family, school peers) of audience that can be reached;
- (c) the inability of targets to entirely eradicate malicious content in some cases; and
- (d) the expense and difficulty (as outlined above) of prosecuting even very serious online offences.

(32) It is therefore worth considering whether these Acts need updating, or whether we actually need a new Online Communications Act that specifically covers the increasing range of abusive behaviours on the internet.

(33) This difficulty is further exacerbated by a culture in which offline crime still seems to be seen as more serious than any supposed online counterpart. For instance, the CPS provides useful guidance on behaviours such as stalking,¹⁸ harassment,¹⁹ and school bullying,²⁰ but if one reads these guidelines, it seems that the offline version is considered the norm, and any online variant, where it is even acknowledged to exist, is simply considered a sub-type.

(34) This overlooks the fact that supposedly equivalent behaviours like cyberstalking, cyberharassment, and cyberbullying can have their own unique attributes, methods, and consequences which require dealing with in fundamentally different ways. Indeed, what little the CPS has to say about online antisocial behaviours tends to be vague.²¹

(35) In short, it appears that we need CPS guidance for the police, court system, legal practitioners, etc. that would provide definitions for, and explanations of the various antisocial online behaviours (eg trolling, cyberbullying, cyberstalking, etc), and information with regards to issues of jurisdiction and proof.

(36) Finally, across the European Union, the Safer Internet Programme²² is promoting self-regulation,²³ and already, several high-profile corporations have signed up to a set of Safer Social Networking Principles.²⁴ This is a great start, but these principles are purely voluntary, and whilst it would be inappropriate to enforce such principles across all EU-based social networks, it is worth returning to the example of Ms Smith, and to ask whether those profiting from social networks should have similar duties of care towards their site users.

CONCLUSION

(37) The full potential of the internet is yet to be realised. If we are to fully enjoy the benefits, and reduce online threatening and abusive behaviour, my belief is that we must approach this in a comprehensively and holistically. I hope the above may offer some ways in which to achieve this.

September 2013

¹⁷ www.cps.gov.uk/consultations/social_media_guidelines.pdf

¹⁸ www.cps.gov.uk/legal/s_to_u/stalking_and_harassment/#a02b

¹⁹ www.cps.gov.uk/legal/s_to_u/stalking_and_harassment/#a02a

²⁰ www.cps.gov.uk/legal/v_to_z/youth_offenders/#a25

²¹ www.cps.gov.uk/southwest/cps_southwest_news/news_articles/in_the_dock_prosecuting_cyber_bullying_electronic_stalking_and_trolling/

²² <http://ec.europa.eu/digital-agenda/self-regulation-better-internet-kids>

²³ <http://ec.europa.eu/digital-agenda/self-regulation-better-internet-kids>

²⁴ http://ec.europa.eu/digital-agenda/sites/digital-agenda/files/sn_principles.pdf

Further written evidence submitted by Dr Claire Hardaker

This is a brief note to add to a previous document submitted to the Culture, Media and Sport Committees inquiry into Online Safety. In brief, the CASS Centre at Lancaster University was successful in their bid for ESRC funding on a project that aims to investigate the rape threats sent by Twitter trolls to a number of high profile women (ES/L008874/1). The project will investigate what the language used by those who send rape/death threats on Twitter reveals about...

1. Their concerns, interests, and ideologies; what concept do they seem to have of themselves and their role in society?
2. Their motivations and goals; what seems to trigger them? What do they seem to be seeking?
3. The links between them and other individuals, topics, and behaviours; do they only produce misogynistic threats or do they engage in other hate-speech? Do they act alone or within networks?

We're hoping that this project will offer timely insight into an area where policy, practice, legislation, and enforcement is currently under intense scrutiny and requires this type of research to help shape future developments. As such, we would be pleased to pass on the results of this project as they come in, and it goes without saying that we would be delighted to also make available all of the final, official findings, reports, articles and so forth at the end of the project.

October 2013

Written evidence submitted by the Remote Gambling Association

INTRODUCTION

1. The Remote Gambling Association ("the RGA") has noted that the Culture, Media and Sport Committee has decided to investigate a number of aspects of online safety that are currently raising concerns, in particular how best to protect minors from accessing adult content. We would, therefore, like to set out the experience of the online gambling sector and the success we have achieved in addressing a number of key risks.

2. By way of introduction, the Remote Gambling Association (RGA) is the largest on-line gambling trade association in the world, representing the world's largest licensed and stock market-listed remote gambling operators and software providers. The organisation provides the remote gambling industry with a single voice on all issues of importance to regulators, legislators, and key decision-makers. Our members are listed on our website which is www.rga.eu.com.

3. The members of the RGA are committed to the protection of young and vulnerable people. We promote responsible gambling and have worked with regulators and legislators to ensure that the rules affecting gambling are both workable and proportionate to the harm that could be caused.

WHY REGULATED REMOTE GAMBLING IS DIFFERENT TO OTHER "ADULT" PRODUCTS

4. The Gambling Act 2005 allowed for a wider range of advertising of gambling products in Great Britain. To be able to advertise a gambling operator has to hold an operating licence issued by the Gambling Commission, or an equivalent licence issued by an EU gambling regulator or an overseas regulator which issues licences with equivalent standards to the UK regulator. These licences require that before bets can be settled the customer is over 18 and has had his or her identity verified.

5. As far as we are aware, no other adult service providers are required by law to ensure that their customers are over the age of 18. This puts the regulated online gambling industry in a different position to other e-commerce sectors. because there are mandatory safeguards in place, but especially where children are concerned we believe that the principles at least should be applied equally.

THE CURRENT REQUIREMENTS FOR LICENSED ONLINE GAMBLING OPERATORS

6. The requirements of the licences held by our members mean that all operators require customers to open accounts. As part of this process their identity and age will be verified.

7. UK and similar legislation around Europe that applies to online gambling requires very high standards of age verification and it is commonly an offence to knowingly accept bets from minors. We support this position and have proactively worked with third party suppliers to improve the range and reliability of data that is used to identify whether someone is under 18 or not.

8. In practice this means that during the account opening process potential customers are asked to provide a range of information and, amongst other things, this is checked by third parties (such as Experian) to confirm the customer's identity and payment details. Details will be checked against any databases (public or private) to which they have access and they will see whether the applicant has a credit history, which of course will not be the case for children.

9. Under the Gambling Commission's Licence Conditions and Codes of Practice, customers will not be able to withdraw any winnings until the age verification process has been satisfactorily completed. In any event, if the customer has failed to satisfactorily complete the age verification checks within 72 hours of registering a relevant bank card and placing their first bet, the operator will freeze the account, prevent the customer from gambling any further until they have satisfactorily completed these checks and, if upon completion of age verification the customer is ultimately shown to be underage, the operator will return all stakes to the young person.

10. In practice the necessary checks for the vast majority of account applicants can be undertaken almost immediately, but the 72 hour window mentioned above allows companies if required to seek documentary evidence of identity and age if the electronic verification does not provide the right level of assurance.

11. There are occasionally cases where people allege that a child has opened an account in their name or has illegally used the existing account of an adult. In reality this happens very rarely and always comes to light when funds are withdrawn from the adult's bank account (and even then it presupposes that the minor has knowledge of the requisite passwords etc in order to gain access). If someone believes that their credit or debit card has been used fraudulently they should contact the operator and their bank and then the cardholder will be able to challenge the charges made, in exactly the same way they would if the card had been used to purchase other goods or services. Although we would suggest strongly that there should be a greater element of parental control in these situations, if it can be proven that the bets were placed by someone who is under 18 then the bets will be cancelled and stakes returned (see para 9 above).

12. With regard to advertising, only suitably licensed operators are able to market gambling products in the UK. This provides another safeguard and all advertising, irrespective of where the operator is based, must comply with the relevant requirements from the Advertising Standards Authority and OFCOM which have clear and enforceable rules to prevent the targeting of advertisements at minors. In addition, the British gambling industry's own advertising code of practice has put in place further protections, including the 9.00pm television watershed, for all gambling except for betting around live events and bingo. It all bans any form of gambling sponsorship from appearing on children's products.

ONLINE GAMBLING AS AN EXAMPLE OF REGULATORY BEST PRACTICE OF ONLINE CHILD PROTECTION

13. In July 2011 the European Commission sought views on these issues as part of its consultation on a Green Paper on Online Gambling in the Internal Market.

14. Some of the questions asked how on-line age controls are imposed. A response was submitted by the Children's Charities' Coalition on Internet Safety, which includes Action for Children, Barnardo's, BAAF, The Children's Society, NCB and NSPCC. Their response stated:

"Since the online age verification laws came into force in the UK in September 2007, the children's organisations have not been made aware of a single instance where a child has beaten the system and got online to gamble. There have been instances where a child has 'borrowed' a parent's credit or debit card and has been able to pass themselves off as the parent, but that raises different issues. There is nothing that laws can do about that, neither is there an easily foreseeable technology fix that can solve it. However, we are not aware of any instances where a child was able to lie about their age and get away with it in an online environment, as they used to do quite easily before the law was changed. By comparison it may not be so difficult to 'PhotoShop' a fake ID to use in a real world setting.

The law should never require an online gambling [operator] to get everything 100% right 100% of the time. That is impossible. But society is entitled to expect gambling web sites to be able to demonstrate that they are making reasonable efforts. Asking someone to tick a box to confirm their age, without more, is not reasonable. It is negligent."

15. On the 23 November 2010 Claire Perry MP speaking in an adjournment debate on the topic of Internet Pornography in the House of Commons looked to the controls on the online gambling industry as an example of how age verification works. She said:

"The previous Government sensibly introduced workable age-verification restrictions on online gambling sites in 2005, an excellent model that works well and searches financial and electoral databases to verify that users are old enough to enter the site and engage in the gambling within. It is a workable model, the previous Government introduced it, and they are to be commended for doing so."

16. In September 2008 the European Commission held a forum on Cross Media Rating and Classification and Age Verification Solutions. The subsequent report stated that:

"the British model, restricting access to online gambling sites [is] seen as the most effective in preventing access to sites using these technologies."

17. There are other examples that could be cited, but we hope these will suffice to show that the success of these measures is not something that the online gambling industry is merely claiming.

18. Following on from this, we believe that the legal requirements to ensure that all people gambling are over the age of 18 are the most appropriate controls for the online gambling industry. We believe that the requirements to age verify online gamblers works. There is very little evidence that young people are attracted to, or participate in remote gambling.

ARE YOUNG PEOPLE ATTRACTED TO ONLINE GAMBLING?

19. There should never be any complacency about the issue of under-18s and gambling, however, in assessing what the most proportionate controls should be it would be wrong to assume that there is a huge interest in this activity.

20. The only significant reference we have been able to find on whether young people are particularly attracted to on-line gambling is in Professor Gill Valentine's report "Literature review of children and young people's gambling" (September 2008). In that she stated "To-date there is not enough evidence to assess whether the advertising/promotion of gambling—including free demonstration games available on websites—has a direct effect on gambling participation." While she recommended that further research is undertaken no such research has been completed as at August 2013.

21. The main research undertaken into the prevalence of gambling among young people has been undertaken on behalf of the National Lottery Commission. As the legal age for participation in the National Lottery is 16 the research they have undertaken is on people aged 15 and under. The most recent research conducted by Ipsos MORI and the Social Research Institute published in July 2012 showed that 18% of 11–15 year olds say they have gambled in the past week. Rates of participation in online gambling are lower than rates of involvement in offline gambling. Thirteen per cent of children say they have played free online gambling games; this is most often through Facebook. Seven per cent of children aged 11–15 say they have some experience of playing online gambling games for money, although around half of this can be explained by children playing alongside parents, with their parents' permission.

FURTHER PROTECTIONS THAT COULD BE PROVIDED TO CHILDREN AND THEIR PARENTS

22. *Advertising:* a review could usefully be undertaken to consider which of the advertising rules that apply to gambling might be extended to all adult products and whether certain rules should be more product-specific. In saying that we are mindful of the high levels of compliance where such rules are in place. From a gambling perspective there has been close engagement by the industry with the ASA in the development of codes. In 2009 the ASA reviewed compliance by the gambling industry with the CAP and BCAP codes and found "*fewer than 1% of the gambling product advertisements [...] seemed to breach the Code, an exceptionally high compliance rate*".

23. *Raising awareness amongst parents:* in order to participate in gambling on a regulated gambling website, customers have to open an account and have their age and identity verified. Although it is not a major problem in terms of the number of cases, a weakness in the system is where a child uses their parent's identity and legitimate credit or debit card to open or use an account.

24. It is self-evident that if this can happen with gambling then it can happen with other adult products. Parents need to understand that they should keep their credit or debit card, password and pin numbers details safe at all times and to supervise the use of credit cards for online shopping. For example if a parent allows a child to use a credit card to purchase a non-age restricted product such as a book they should ensure that the child returns the credit card to them and ensure that the card number is not retained by the child.

25. We also note and support proposals that have previously been made to promote awareness about the parental controls that are available for internet-enabled devices.

26. *Highlighting tools for parents to use:* The RGA has produced technical guidelines to raise standards among industry operators and regulators. As part of its work on responsible gambling it has included the following in that document:

"The operator's responsible gambling page should provide a link to a recognised filtering programme to assist customers/parents in preventing underage individuals from using gambling sites."

27. This provision has been adopted into licences issued by UK and European regulators and is now the industry standard. It is a practical tool for restricting child access to unsuitable sites, but is not in any sense burdensome for operators and, again, could be used for all sites offering adult products.

CONCLUSIONS

28. As an industry which is subject to statutory regulation involving an adult product it is right that expectations and compliance should be high. However, this has led to the industry proactively seeking out and devising practical measures to achieve the regulatory objective of preventing under-18s from accessing gambling products.

29. Experts in child protection have endorsed those efforts and, most importantly, their effectiveness. Although it may not be appropriate to set the bar at such a high level for non-regulated industries, we do feel that there might be lessons to learn from what we have done.

30. As ever, if it would be at all helpful we would be very willing to expand on any of the points made in this letter,

September 2013

Written evidence submitted by Ann Farmer

I would like the Committee to take into account the dangers of online pornography to children and young people, especially in negatively affecting them mentally and emotionally.

My research into eugenics and population has found a significant overlap between these movements and the campaign for “value-free” sex education; both movements have historical links with the pornography industry.

The aim of the pornography industry is to maximise profits by turning people into sex addicts, searching for sexual material on a regular basis, often of an increasingly extreme nature. Eventually they may seek more extreme “thrills” by acting out what they have seen online: two recent cases of rape and murder of young girls, April Jones and Tia Sharpe, have featured the use of pornography by men unknown to police.

There is also evidence that young boys are themselves becoming child molesters, acting out the pornographic scenarios they have seen online.

Pornography dehumanises women and children, depicting them as sex toys to be used at will, often in a brutal manner; even those women who participate willingly do not remain psychologically unharmed. It also dehumanises the viewers of pornography, reducing them to their sexual appetites, and encouraging them to believe that there is a “right to sex”.

Even without these extreme negative outcomes, we must face the prospect of a society where the younger generations have learned to view other people through the distorted prism of a perverted sexual desire; the history of pornography shows that lust swiftly turns to cruelty, thus we must tackle this problem of easily accessible online pornography if we do not wish society to be composed increasingly of uncaring sociopaths who care chiefly about their own sexual appetites.

September 2013

Written evidence submitted by Kirsty Hopley

Online pornography is free, easily accessible and the content is extreme. Anyone can access any type of pornography including, violence, rape, acted child pornography, s and m, extreme degradation of women and more. There is no log in page and no age check. This is unacceptable. This is not tolerated in pubs or strip clubs so why is it freely available online? A simple answer is to make online pornography sites operate account only sites, the user must provide their details and have a user name. This will reduce the amount of times people stumble upon online porn without affecting the freedom of choice for users of online porn.

Secondly, internet filters are great for parents and I am in favour of the automatic filter. It makes sense that those who wish to view pornography should be the ones making the choice rather than everyone getting it and then having to choose not to have access. However, there are serious concerns.

I have Talk Talk Homesafe settings which are good in theory. They allow the user to turn on and off filters. In practice this rarely works. I need to turn filters off to read material for my work but usually when I want to turn it back on, it freezes or takes hours. Secondly, some sites are blocked which do not contain pornography such as rape support sites. Similarly, even with my homesafe settings on I could still type in sex or porn and get some extreme sexual images through google images. It is crucial that this is monitored and dealt with swiftly. Clearly the technology is already there, it just needs monitoring.

Next issue is advertising. Many sites have pop ups which can lead to sexual material. I have seen instances of this on school approved websites and on kindle children's books (Alice in Wonderland was one). Advertising that is aimed at adults should never appear on sites that are aimed at children. This should be a criminal offence as it is grooming.

Online safety is something parents need to understand to take seriously. With channels such as Ceebees encouraging very young children to go online and the rise of little children having tablets, education of parents is key. My suggestion is that this is discussed by Health Visitors in the early years checks. It should be a face to face discussion of the dangers and a leaflet given of how to keep up. Every device that is sold must have an easy to understand guide for parents to set blocks and this should be discussed at purchase. This needs to be regulated so that it happens every time. It is not like the days when parents had to make sure toddlers didn't choke on a piece of lego, parents do not understand the technology that their kids do. The digital age has

approached so quickly. Following this, schools should offer compulsory help for parents to understand keeping children safe online. The world has moved on and parenting needs to catch up.

This is an issue which the government needs to support parents to protect children. The starting point is to regulate the porn industry (like we do with tobacco, alcohol and gambling industries). It is unbelievable that the porn industry is given such a free reign to provide such an unrealistic and harmful portrayal of what is actually a wonderful act that humans should enjoy.

September 2013

Written evidence submitted by Dr Peter Nelson

PORNOGRAPHY: BRITAIN'S BIG PROBLEM

A young man walks into a newsagent and buys a copy of the *Sun* or similar newspaper. On page 3, he sees a picture of a young woman wearing little or no clothing. What goes through his mind?

Does he think, "I must get a good job, earn a living, save some money, get married, have children, and help bring them up"?

Or does he think, "I must go out at the weekend, have some drinks, find a woman, and have sex with her"?

If the latter is the case, then society has a big problem.

CONSEQUENCES

In the *first* place, young men who think like this do not make good fathers. They make women pregnant, but take little or no interest in bringing up the children. This leaves women bringing up children on their own. While some do this remarkably well, the evidence is that children from single-parent families do less well, and are less well-behaved, at school.¹ Even in homes where a father is present, there can be domestic violence which has an adverse effect on children. Many of the problems in education today can be traced back to poor parenting. Teaching youngsters who lack discipline and encouragement to study is very difficult.

Secondly, the open display of sex in the media brings sex to the attention of children from an early age. This leads them to engage in sexual activities before they are old enough to appreciate the consequences. Teenage pregnancy rates in Britain are very high. This is despite attempts to bring them down by promoting the use of contraceptives in schools.² These fail because they raise children's interest in sex still further. Even good sex education is limited in what it can do, given the big influence the media have on young people.

A recent NSPCC study reveals that nine out of ten young people between 13 and 17 years old in England, Scotland, and Wales have experienced some form of intimate relationship.³

Thirdly, pornography encourages men to be promiscuous. Promiscuity leads to transmission of sexually transmitted-diseases (SDIs). Health agencies promote the use of condoms to try to stop this, but condoms are not always used, and frequently fail. SDI levels in Britain are very high and rising. The number of new diagnoses in the UK is now running at 1.3% of the population per year.⁴

Fourthly, pornography inflames men's sexual passions. Men who cannot control these may attack women. The incidence of rape and indecent assault on women in Britain is very high. On present figures, one in ten women will be raped or assaulted during their lifetime.⁵ The NSPCC study referred to earlier found that as many as one in three girls in Britain have experienced some form of sexual violence from a partner.³

Adult pornography may also be implicated in the development of paedophilia.⁶

Fifthly, sexual images of women contribute to the pressure on men to assert their masculinity. They see women vaunting their sexuality and want to show off theirs. This leads them to engage in loutish behaviour, drink heavily, drive recklessly, and so on. Anti-social behaviour is a big problem in Britain today, and much of it is macho-driven.

Sixthly, pornography contributes to mental illness in society. Many mental problems have a sexual component. Emotions are interconnected, and difficulties in one area can lead to problems in another. Some men have so much difficulty coping with pornography that they have set up a help group, "Men and Porn". Many suffer on their own, and are reluctant to admit that they have sexual problems. The incidence of mental illness in Britain today is very high and rising.

While most pornography is aimed at men, it encourages women too to think of sex as something to be pursued as an end in itself, and not just as part of a stable relationship within which children can be brought up. Pornography aimed at women will do this even more.

PROOF

The contribution of pornography to these various problems is evidenced by the extent to which they have grown over the last sixty years. Sixty years ago, media standards were high, and there was almost no

pornography on sale to the public. Since then, standards have been relaxed, and the volume and explicitness of pornography have increased. At the same time, the incidence of all the above problems has grown.

This is shown by the following comparisons, taken from my 2005 briefing paper.⁴ There are large rises in all the indicators from the 1950s to the 2000s.

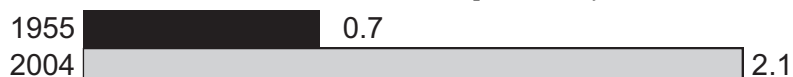
Teenage pregnancies

The following chart compares the number of girls in England and Wales becoming pregnant below the age of 14 per thousand members of their age group.



Sexually-transmitted infections

The chart below compares the number of new cases of syphilis, gonorrhoea, herpes, and genital warts in England and Wales per thousand members of the population. The comparison is limited to these STIs because there was no HIV/AIDS in the 1950s, and no records were kept of chlamydia or other infections.



Sexual crime

The following chart compares the number of rapes and sexual assaults on women and girls per thousand members of the female population. This is based on the number of offences reported to the police. Reporting of sexual crimes against women has become easier since the 1950s, but against this, many women take protective measures that they did not take then (eg avoiding going out alone at night).



Family breakdown

Sexual infidelity is one cause of family breakdown. (Other factors are money, alcohol, and drugs.)

The chart below gives the number of lone parents with dependent children in Britain as a percentage of the total number of families with dependent children.



Mental illness

Sexual problems are one cause of mental illness. A measure of the level of mental illness in society is the number of anti-depressant drugs people use. The following chart compares the number of prescription items for these drugs in the community in England per person. Anti-depressants were introduced in 1957.



Macho violence

Much of the violence in society is driven by machismo. Alcohol is often implicated, but heavy drinking by men is itself, in many cases, macho-driven. Violence in the media and drugs are other factors.

The chart below compares the number of violent offences against the person recorded by the police in England and Wales per thousand members of the population. The comparison is only very approximate because the police have changed the way they count violent crimes. I have doubled the 1955 figure to allow for this.



This evidence leaves little doubt that pornography is very harmful. This finding contradicts the conclusions of Home Office reports on the effects of pornography, published in 1979 and 1990.⁷ I have discussed the

weaknesses in these reports elsewhere.⁸ The biggest one is that they do not answer the question, “If pornography is not a major cause of the sexual problems now afflicting society, *what is?*”

A more recent study of hard pornography by the Ministry of Justice concludes that this *does* have a harmful effect on adults.⁹ Other recent studies, including one by Dr Linda Papadopoulos for the Home Office, similarly conclude that exposure to pornography has a harmful effect on children.¹⁰ Dr Papadopoulos’ report is alarming. Would that the proponents of permissiveness in the 1960s had heeded the warnings of those who predicted what the consequences of this would be.

REMEDY

The remedy for these problems is for the Government to enact legislation to restore standards in the media to where they were sixty years ago. This will be difficult. Users of pornography will protest, and liberals will complain about loss of freedom. The above problems are, however, huge and need to be addressed.

My suggestion is that the Government sets up a Royal Commission to re-examine the effects of pornography and to make recommendations. Acting on a Royal Commission’s report would be easier for Government than acting on its own.

I have answered objections to raising standards and discussed possible legislation elsewhere.¹¹ The answer to the objection of loss of freedom is that pornography takes away even more freedom—from women who would like to be able to go out alone at night, from young mothers who would like to do what their other friends do, from men who find pornography addictive, from old people shut in for fear of macho-driven yobs, and so on.

Pornography makes for a less civilized society. It is an evil, and needs to be treated as such.

REFERENCES

1. Lords and Commons Family and Child Protection Group report 1998.
 2. Cf. M Henderson *et al*, “Impact of a theoretically based sex education programme (SHARE) delivered by teachers on NHS registered conceptions and terminations: final results of cluster randomised trial,” *BMJ*, 2007, **334**, 133; Meg Wiggs *et al*, “Health outcomes of youth development programme in England: prospective matched comparison study,” *BMJ*, 2009, **339**, b2534.
 3. Christine Barter *et al*, *Partner Exploitation and Violence in Teenage Intimate Relationships*, NSPCC, 2009.
 4. P G Nelson, *Sex in the Media: Is it Harmful?* mediawatch-uk, 2005.
 5. Andy Myhill and Jonathan Allen, *Rape and Sexual Assault of Women: the Extent and Nature of the Problem*, Home Office Research Study 237, 2002.
 6. P G Nelson, *Nudity and Sexual Activity in the Media*, Whittles, 1998, Sect. 1.5.2.
 7. Report of the Committee on Obscenity and Film Censorship, chairman Bernard Williams, 1979; Dennis Howitt and Guy Cumberbatch, *Pornography: Impacts and Influences*, 1990.
 8. *Nudity and Sexual Activity in the Media*, Chap. 2.
 9. Catherine Itzin, Ann Takets, and Liz Kelly, *The Evidence of Harm to Adults Relating to Exposure to Extreme Pornographic Material*, Ministry of Justice Research Series 11/07, 2007.
 10. Michael Flood, “The harms of pornography exposure among children and young people,” *Child Abuse Review*, 2009, **18**, 384; Linda Papadopoulos, *Independent Review into the Sexualisation of Young People*, Home Office, 2010.
 11. *Nudity and Sexual Activity in the Media*, Chaps. 3–4.
- September 2013

Written evidence submitted by the British Board of Film Classification

EXECUTIVE SUMMARY

- The British Board of Film Classification (BBFC) is the UK’s regulator of film and video. The BBFC’s primary aim is to protect children and other vulnerable groups from harm through classification decisions which are legally enforceable and to empower consumers through content information and education.
- Although the ecology of the internet is different from that of the more regulated offline environment, the risk of harm, particularly to minors, from both legal and illegal material is at least as great online. Government, industry and regulators should work together to reduce the harm risk wherever possible. There is a case for more joined up co and self-regulation online drawing on existing, effective, and often industry-led models, encouraged and supported by Government.

- The starting point for co- and self-regulatory models to protect children online should be clarity of approach and consumer and industry support. The BBFC sets out in its submission the factors for the success of online co- and self-regulatory systems: child protection at its core; effective labelling of content; broad coverage; low cost; efficient, flexible and innovative.
- The BBFC is ready to continue to make available its expertise and experience, working with Government, industry and other regulators to improve child protection online. Examples of the BBFC's involvement in this area include:
 - voluntary self-regulation by the BBFC of Video-on-Demand (VOD) content applying granular age ratings and content advice;
 - the BBFC-run regulation of mobile content, including websites, using a binary classification system based around the BBFC 18/R18 standard which enables the filtering of content and protection of minors; and
 - development by the BBFC and NICAM of a User Generated Content (UGC) ratings tool. This self-regulatory questionnaire is tailored to reflect national differences and is designed to be completed by those uploading the content or the audience, allowing the use of online filters to prevent children accessing inappropriate content and the facility to report abuse.
- Online pornography is an important example of where co or self-regulation has not worked well. The BBFC removes any material from pornographic works it classifies which is potentially harmful or otherwise illegal under the Video Recordings Act (VRA), including so-called "rape porn". But online, where the VRA and its harm test do not apply, harmful material including "rape porn" is available. Greater regulation of such adult content, and content which the BBFC will not classify at any category, would be welcome for the better protection of minors.
- There are some obvious areas where Government intervention may be appropriate to better protect children online. Lack of industry self-regulation of online pornography is leading to children being able to access inappropriate and potentially harmful content. Equally, industry could do more, for example through effective moderation or through the age rating of online music videos, to ensure that their service is safe for children and the vulnerable online.

1. INTRODUCTION

1.1 The British Board of Film Classification (BBFC) is grateful for the opportunity to respond to the Culture, Media and Sport Committee Inquiry into Online Safety.

1.2 The BBFC is an independent, non-governmental body which classifies films and videos distributed by way of packaged media and, increasingly, on the internet. The BBFC's primary aim is to protect children and other vulnerable groups from harm through classification decisions which are legally enforceable and to empower consumers, particularly parents and children, through content information and education. The BBFC will not classify material which is illegal in the UK, including content which promotes terrorism or which features indecent images of children. The BBFC became the independent regulator of content delivered by mobile networks in the UK from 2 September 2013. The Director of the BBFC, David Cooke, sits on the Executive Board of UK Council for Child Internet Safety (UKCCIS) in recognition of the BBFC's role in the protection of children online.

1.3 The BBFC classifies films and videos/DVDs according to its Classification Guidelines, with ratings ranging from U for Universal to R18 which are restricted videos only allowed to be sold in licensed sex shops. The BBFC's Guidelines are the result of extensive public consultation with over 10,000 people across the UK being consulted during the most recent Guidelines consultation in 2013. Research demonstrates that the public agrees with the BBFC's classification decisions most of the time. 92% of recent film viewers agreed with classification of films they had seen recently. (*Goldstone Perl, Bernice Hardie 2013*); and recognises and understands the BBFC's symbols 89% of the time (rising to 97% for parents) (*TNS, 2007*).

1.4 The BBFC also publishes (on its website and Apps) more detailed information, BBFCinsight, aimed primarily at parents, which outlines the key content issues in a film and thereby enables viewers to make fully educated viewing decisions for themselves and their families. This information is available both when the content is distributed by way of packaged media and online. Independent research (*Slesenger, 2009*) suggests that 86% of parents of primary schoolchildren find this information useful.

1.5 The BBFC runs an extensive education programme both online and through a series of seminars at the BBFC and throughout the country, with visits to schools and colleges, speaking to over 12,000 students in 2012 on media literacy and the classification process. The BBFC further contributes to a number of media literacy initiatives run by industry and child protection groups, including Childnet UK, advising children and adults on how to keep themselves and their family safe online.

2. THE BBFC AND HOME ENTERTAINMENT INDUSTRY SELF-REGULATION ONLINE

2.1 For historical reasons, the current statutory regime for film and video/DVDs does not cover online content. The Video Recordings Act was originally passed in 1984 before digital downloads of videos/DVDs. However, media convergence is increasingly blurring the distinction between physical and online material.

2.2 Independent research commissioned by the BBFC shows that while the public considers that the internet brings greater choice, freedom and flexibility, the majority of viewers still consider it important to be able to check the suitability of audio-visual content they download. 85% of the public consider it important to have consistent BBFC classifications available for Video-On-Demand (VOD) content; rising to 90% of parents of children under 16 (*Bernice Hardie, 2011*).

2.3 In recognition of public demands for regulatory protection online, the BBFC has worked in partnership with the home entertainment industry on a number of voluntary, self regulatory services which bring trusted BBFC classification standards and well known age ratings and symbols online. BBFC digital services offers labelling and content advice services designed for content providers and platform owners (digital video services). These services cover all forms of video-on-demand including subscription models (SVOD) and transactional (TVOD).

2.4 The BBFC has now rated more than 200,000 videos for online distribution by such companies as Warner Bros, Walt Disney, 20th Century Fox, Paramount, Universal, Sony; with BBFC ratings used by platforms such as iTunes, Netflix, Blinkbox/Tesco, Sainsbury's, Dixons, BT Vision and Talk Talk. The new industry initiative known as UltraViolet—which promotes the digital ownership of content—is also working with the BBFC. Displaying BBFC labelling enables consumers to make informed choices when purchasing retail and rental digital video, thereby empowering parents to protect their children.

2.5 BBFC digital services include a ratings service aimed specifically at content that is only available online and that would otherwise not be provided with a rating. This service—known as Watch and Rate—is becoming more popular and well-used. Compared with the same period in 2012, there has been a 141% increase in industry take up as of 10 September 2013.

3. ONLINE PORNOGRAPHY

3.1 It is generally accepted that exposing children to pornography is potentially harmful to them and is likely at the very least to impair their development. This is why many countries, including the UK, have enacted measures to prevent children from accessing pornography.

3.2 In the UK, the BBFC classifies all pornographic content released both on video and theatrically. The BBFC removes any material from pornographic works which is potentially harmful or otherwise illegal. As well as policing the border between legal and illegal pornography, the BBFC polices the border between the strongest, hardcore pornography, and the less strong, softcore pornography. The BBFC classifies hardcore pornography as R18, which means that it may only be supplied through licensed sex shops, as an extra precaution against underage viewing. However, the risk of children accessing even the strongest legal pornography is far greater online. In addition, there are fewer effective controls on the distribution online of pornography which the BBFC would not classify at any category.

3.3 Online pornography is an important example of where co or self-regulation has not worked well. While the majority of the home entertainment industry has chosen to opt for voluntary self regulation, no members of the adult industry currently use the BBFC's digital services. The market imperatives which in the UK have driven the mainstream home entertainment industry to adopt best practice self regulation, work in the opposite direction in relation to adult content. While the mainstream video industry recognises that parents want the reassurance of trusted labels on online content, much of the adult industry wants to advertise its product as "uncensored".

3.4 The BBFC removes any material from pornographic works it classifies which is potentially harmful or otherwise illegal under the VRA, including so-called "rape porn". The BBFC intervenes to remove from a pornographic work any portrayal of sexual activity which involves lack of consent, whether real or simulated. The BBFC will also remove material, including dialogue, which is likely to encourage an interest in sexually abusive activity, including rape. In short, "rape porn" does not exist in works classified by the BBFC. But online, where the VRA and its harm test do not apply, "rape porn" is available. The BBFC believes that consideration needs to be given into how protections that are applied to physical R18 material can also be applied online if much of the adult industry continues to refuse to participate in self-regulatory measures. The BBFC therefore welcomes the Prime Minister's declaration on 22 July 2013 that Government will ensure:

"that videos streamed on line in the UK are subject to the same rules as those sold in shops. Put simply—what you can't get in a shop, you will no longer be able to get online."

3.5 The Government has recognised the dangers of extreme pornography and in 2008 made possession of extreme pornography an offence under the Criminal Justice and Immigration Act. A BBFC classification is a defence against a prosecution under this Act therefore purchasing a legally classified work is a protection against inadvertently possessing extreme pornographic material. The BBFC regularly assists Local Government trading standards officers in ensuring that pornographic material has been classified by the BBFC and restricted for sale to licensed sex shops. However, these methods of enforcement are not available online.

3.6 While physical video works rated R18 by the BBFC may only be supplied to adults through licensed sex shops, restrictions to prevent children accessing such material are not maintained online, except for UK services regulated by the Authority for Television On Demand (ATVOD). These services form a very small proportion of the market, making it easier for those under 18 to access potentially harmful pornography. In

addition, ATVOD can only intervene and impose rules to require that the material must be made available in a manner which secures that children will not normally see or hear it, if a programme distributed online by a UK provider contains material which might seriously impair the physical, mental or moral development of persons under the age of 18.

3.7 The BBFC believes that there is a case to strengthen the definition of content online likely to seriously impair the development of minors so that it is clear that hardcore pornography constitutes such content. One option might be an amendment to the Audiovisual Media Services Directive so that explicit depictions of real sexual activity, or activity involving realistic infliction of pain or injury, or real or simulated lack of consent to sexual activity, must be provided in such a manner which ensures that under 18s cannot normally see or hear it. Such an approach would be consistent with that in the Government's paper: *Connectivity, Content and Consumers: Britain's digital platform for growth*.

4. THE BBFC AND MOBILE NETWORKS' SELF-REGULATION OF ONLINE CONTENT

4.1 From 2 September 2013, the BBFC became the independent regulator of content delivered via the UK's four main mobile networks (EE, O2, Three and Vodafone). Under this new self regulatory system, the BBFC has created a Classification Framework, based on the trusted, transparent and consistent standards set out in its Classification Guidelines, which specifies what content should be placed behind access controls/filters. The Classification Framework is a living document which will be updated regularly to reflect evolving public attitudes and societal concerns.

4.2 The standards in the BBFC's Classification Guidelines are used to ensure content which would be age rated 18 or R18 by the BBFC will be placed behind access controls and internet filters by mobile operators to restrict access to that content by those under 18. This content includes pornography and other adult sexual content, pro-smoking and pro-Ana (anorexia nervosa) websites and content which promotes or glorifies discrimination, drug misuse or real life violence. The BBFC and the mobile operators believe that this partnership will be trusted by the public, more transparent than the previous mobile regulatory regime and better able to adapt to changes in societal attitudes and concerns in relation to child protection.

4.3 The BBFC believes that child protection would be improved if those operating public WiFi services in places regularly visited by minors applied the same, consistent standards as those used by the mobile operators. The BBFC would be able to offer assistance in setting and applying these standards, as it has done in partnership with the mobile operators for content accessed via mobile networks.

5. USER GENERATED CONTENT ONLINE

5.1 The BBFC was a third party member of the EU's CEO Coalition to make the Internet a better place for children. In response to a call for action from the European Commission, members of the Coalition in 2012–13 undertook to take positive action to make the Internet a better place for children in the European Union. The Coalition aimed to make the internet safer for children and the vulnerable through action in five core areas: simple and robust reporting tools, age-appropriate privacy settings, wider use of content classification, wider availability and use of parental controls and effective takedown of child abuse material.

5.2 In response to this initiative, the BBFC and its counterpart, the Dutch regulator, the Netherlands Institute for Classification of Audio Visual Media (NICAM) together developed a tool for ordinary people to age rate User Generated Content (UGC) across different countries and platforms and according to recognised and trusted national standards. UGC is growing in significance and needs to be addressed to allow parents the tools to prevent children and the vulnerable from accessing inappropriate content.

5.3 The UGC tool, using a single, simple, free to complete questionnaire, instantaneously produces an age rating which can be shown on the video hosting platform and linked to internet filters. The ratings differ from country to country to reflect different national concerns over content. For example, strong language is an issue for consumers in the UK but not in the Netherlands.

5.4 The tool is simple to use and understand. It contains six questions about the content of the UGC, on behaviour (including racism and other discriminatory behaviour, self harm and suicide), drugs, horror, language, sex/nudity and violence. Completing the questionnaire takes less than two minutes. It also includes a facility for viewers to report content which in their view is abusive or even illegal, such as material intended to promote terrorism or child sex abuse images.

5.5 The questionnaire is flexible. It may be completed by those uploading content or it may be completed by those viewing the content. The ratings can then be linked to online filters. This new initiative will shortly be trialled by Mediaset in Italy and the BBFC and NICAM are looking for trial partners elsewhere across the EU. This initiative could make the online world safer for children and has been welcomed by the EU Commission's CEO Safer Internet Coalition and the UK Government.

5.6 The BBFC would be happy to demonstrate to the Culture, Media and Sport Committee how this tool could help to make the internet safer for children.

6. MODERATION

6.1 One core area that the BBFC believes could significantly improve child protection online is effective moderation of sites that appeal to children and teenagers. The case of instances of inappropriate behaviour on the site *Habbo Hotel* and Ask.fm demonstrates the importance of robust moderation and effective follow up action if children are to be properly protected.

7. EXEMPTIONS FROM THE VIDEO RECORDINGS ACT AND ONLINE MUSIC VIDEOS

7.1 When the Video Recordings Act (VRA) was passed over 25 years ago certain video works were made exempt from classification by the BBFC because they were considered unlikely to be harmful. The threshold at which music, sport, documentaries and religious works lose their exemption from the VRA remains extremely high despite the content of these exempt works having changed beyond all recognition since 1984. This high threshold has meant that inappropriate and potentially harmful content in such works is exempt from statutory classification, allowing it to be legally supplied to children.

7.2 On 24 May 2013, following a consultation, the UK Government announced that it plans in 2014 to lower the exemptions threshold for all currently exempt material in order to prevent children accessing potentially harmful material. Once implemented, the decision will improve the protection children enjoy from potentially harmful media content by ensuring that video content such as drug misuse, strong violence, racist language, and certain sexual content falling short of actual sex will no longer be legally able to be freely supplied to children. Instead, the BBFC will classify such content to keep it away from vulnerable and impressionable children.

7.3 However, there is particular concern about the content of currently exempt music videos and online music videos, highlighted among others by Reg Bailey in his review into the commercialisation and sexualisation of Children which resulted in the report *Letting Children be Children*. The Government's proposed amendment to the VRA will only bring physical music videos within the BBFC's regulatory ambit. In the Department for Education's Progress Report on the Bailey Review in May 2013, the Government stated:

"On music videos, we want industry to develop solutions no later than the end of the year to ensure online videos—particularly those that are likely to be sought out by children and young people—carry advice about their age-suitability and content."

7.4 The BBFC hopes to work with the recorded music industry towards the goal of achieving well understood and trusted age ratings and content advice for online music videos as we have done successfully with the home entertainment industry in relation to other online videos. One company—Universal Music—has begun to submit long form music video content to the BBFC for online age ratings. A number of platforms which use BBFC ratings through BBFC Digital Services have indicated that they would carry music videos if they were age rated by the BBFC. This would then mean that the ability to download these music videos could be controlled by age related filters which would be an important mechanism for child protection online.

8. CONCLUSION: THE APPROPRIATE REGULATORY ENVIRONMENT TO PROTECT CHILDREN ONLINE

8.1 In a converging media world, it is the content, and not the means of distribution, that is important when considering protection of children. The ecology of the internet is of course very different from that of the offline environment where harm risks are well understood and regulated for. But online, the risk of harm, particularly to minors, from both legal and illegal material is at least as great and in some cases (for example access to legal pornography or pro-self harming and suicide content) arguably greater because of a much greater ease of access.

8.2 In several areas, industry and regulators have worked effectively together to reduce the online harm risk. The initiatives outlined in this response for example, which build on the BBFC's partnerships with, among others, mobile operators, digital video services and content providers, and our cooperative relationships with fellow regulators both in the UK and overseas, demonstrate this. The public should continue to benefit from these initiatives. Drawing on its experience and expertise, the BBFC stands ready to work further with Government, industry and other regulators to continue collectively to improve child protection online.

8.3 The key criteria for any regulation should be clarity of approach and consumer and industry support. The BBFC believes that the public policy priority should be to create an appropriate framework enabling both existing and future effective self, co and statutory regulation to flourish, empowering consumers to inform and protect themselves and their families.

8.4 In the BBFC's experience the key factors for the success of an online regulatory system are:

- child protection at its core;
- effective labelling of content so that the standards are trusted and understood and the symbols used are recognisable;
- broad coverage so that the system creates a known standard; and
- low cost; efficient, flexible and innovative service so that it can keep pace with technological change and not be burdensome on industry.

8.6 The BBFC's own self-regulatory solutions fulfil these criteria and have widespread industry and public support. We would encourage Government to continue to encourage and support these, and other, solutions. However, as is clear from our evidence, there are some obvious areas where more robust Government intervention is required to ensure proper protection of children online, for example online pornography, where currently lack of industry self-regulation is leading to children being able to access inappropriate and potentially harmful content. Equally, industry could do more, for example through effective moderation, to ensure that their service is safe for children and the vulnerable online.

September 2013

Written evidence submitted by Arqiva

SUMMARY OF KEY POINTS AND RECOMMENDATIONS

- Arqiva welcomes the opportunity to respond to the Culture, Media & Sport Select Committee's timely new Inquiry into Online Safety.
- Arqiva believes that children and young people should be able to enjoy the benefits of digital technology and the internet, whilst having the right to be safe online. Indeed, the commitment to ensure child safety online is a matter of grave importance—and should be a shared responsibility between parents, businesses and the wider communications industry including ISPs, web publishers, WiFi providers and government. Therefore, Arqiva is pleased to be a member of the Internet Watch Foundation (IWF) and to have fully engaged with the UK Council for Child Internet Safety (UKCCIS), as well as government; key stakeholder organisations, businesses, retailers and manufacturers on this important issue.
- Children gain access to the Internet from many devices: PCs, smartphones, tablets and games consoles; both their own and those owned by their friends and parents. Many of these devices gain access to the Internet via multiple networks: fixed broadband at home, mobile broadband and Public WiFi outside of the house. In simple terms, there are two main ways of filtering the Internet content presented to children:
 - I. The network can filter content, for *all* users, or for children only, where the network can firmly identify the user and the age of that user.
 - II. The device can be set to filter content, with device passwords to prevent children from changing these filter settings.
- Arqiva believes that *both* measures are required to minimise the adult content available to children. The first would benefit from a consistent approach to content filtering for all Internet access networks that provide service in public places. The second requires education for parents and children, as well as a policy that all devices (and internet access software on those devices) should be supplied with adult content filtering turned on by default.
- Arqiva recommends that government place greater emphasis on internet safety themes across the educational curriculum.
- We believe that policy makers should do more to research and improve online protections for more vulnerable children; define inappropriate content and improve the means for identifying it online. In addition, more research should be conducted to understand the many different ways that children and young people are using internet enabled devices, especially in the home and within social environments.
- We also believe that media and communications companies, including the public service broadcasters, play a key role in educating the public.

ABOUT ARQIVA

Arqiva is a media infrastructure and technology company operating at the heart of the broadcast and mobile communications industry and at the forefront of network solutions and services in an increasingly digital world. Arqiva provides much of the infrastructure behind television, radio and wireless communications in the UK and has a growing presence in Ireland, mainland Europe and the USA.

Arqiva was responsible for UK Digital "Switch-Over"—engineering from analogue television to Freeview—a huge logistical exercise which touched every Parliamentary constituency, requiring an investment by Arqiva of some £630 million and was successfully delivered to time and budget.

Arqiva is also a founder member and shareholder of Freeview (Arqiva broadcasts all six Freeview multiplexes and is the licensed operator of two of them) and was a key launch technology partner for Freesat. Arqiva is also the licensed operator of the Digital One national commercial DAB digital radio multiplex.

Arqiva operates five international satellite teleports, over 70 other staffed locations, and thousands of shared radio sites throughout the UK and Ireland including masts, towers and rooftops from under 30 to over 300 metres tall.

In addition for broadcasters, media companies and corporate enterprises Arqiva provides end-to-end capability ranging from:

- satellite newsgathering (30 international broadcast trucks);
- 10 TV studios (co-located with post-production suites);
- spectrum for Programme-Making & Special Events (PMSE)²⁵;
- playout (capacity to play out over 70 channels including HD); to
- satellite distribution (over 1200 services delivered); and
- Connect TV—who launched the first live streaming channel on Freeview.

Arqiva's WiFi network includes almost every UK airport—and reaches cross the hospitality and leisure sector, providing WiFi to 85,000 rooms in leading hotel chains, and many restaurants, retail chains and shopping centres and local high streets.

Elsewhere in the communications sector, the company supports cellular, wireless broadband, video, voice and data solutions for the mobile phone, public safety, public sector, public space and transport markets.

Arqiva's major customers include the BBC, ITV, Channel 4, Five, BSkyB, Classic FM, the four UK mobile operators, Metropolitan Police and the RNLI.

THE QUESTIONS

KEY, OVERARCHING ISSUES:

- How best to protect minors from accessing adult content;
- Filtering out extremist material, including images of child abuse and material intended to promote terrorism or other acts of violence;
- Preventing abusive or threatening comments on social media.

1. Arqiva welcomes the opportunity to respond to the CMS Select Committee's timely new inquiry into *Online Safety*.

2. Over the past decade the UK's media, broadcasting, telecommunications and technology industries have undergone unprecedented, profound and exciting change. As a result of digitisation, the traditional boundaries between what were once separate universes: Content, Communications and Computing are eroding. Such "convergence" has seen the blurring of boundaries between the media, telecoms and information technology sectors.

3. Technology is becoming an integral part of both modern life and children's lives. According to Ofcom: 90% of children live in a household with access to the internet through either a PC, laptop or netbook;²⁶ whilst 65% of children use the internet "almost every day".²⁷ Young people are increasingly taking part in a wide range of activities online, enabling them to discover and access a wide range of content, connect with their friends and family, as well as offering the potential to create and distribute their own content. Young people are understandably excited, stimulated and motivated by these developments. Indeed, recent research suggests that primary age children are "highly engaged" with digital technology.²⁸ It is essential for policy makers and educators to continue to research and understand the many different ways that children and young people are using internet enabled devices, especially in the home and within social environments.

4. However, as well as bringing exciting new benefits, new forms of communication and emerging platforms bring new opportunities for misuse. Whereas, traditionally, the public service broadcasters were trusted by parents to provide quality viewing and listening content; suitable for children and family/inter-generational viewing and delivered in a linear fashion; and at a suitable time (ie: pre or post-9pm watershed); we have witnessed how in recent years emerging commercial "new media" platforms and social networking, in a largely unregulated space, have exposed young people to a range of new dangers—from the exposure to "adult content", to the phenomena of "cyberbullying", "grooming", "sexting", "self-harm", gaming, gambling, as well as illegal downloading and file sharing, or online fraud.

5. Child safety (online or offline) is a hotly debated issue. As Dr Tanya Byron has noted "*A focus on the most terrible but least frequent risks can skew debate in a direction that sends out negative and fear-based*

²⁵ Such as the wireless cameras operated by the BBC and Sky News, and the radio microphones used in virtually all television production and many West End shows.

²⁶ Ofcom's Communications Market Report 2013

²⁷ This is split across; 38% of 5–7 year olds, 62% of 8–11 year olds, 87% of 12–15 year olds—Ofcom's Children and Parents: Media use and attitudes report (Oct'12)

²⁸ UK Safety Internet Centre—Safer Internet Day—Have Your Say Report February 2013: 86% of 7–11s use some form of online communication tool, such as social networks and virtual worlds (56%), chat functions in online gaming (38%) or using webcams (28%). The internet is crucial for schoolwork, and 94% of 7–11s say they have little trouble finding information for their school work on the internet. Secondary age children are prolific online communicators: 96% of young people age 11–19 use some form of online communication tool, including services such as social networks (74%), emails (72%), instant messaging (68%), webcams (52%), chat functions in online gaming (45%), chat rooms (17%) and blogs (14%). Young people are also contributing to the production of online content: a quarter (24%) of 11–19s have created a website, 21% have created a game, 14% have created an app and 12% have created a blog

messages to children, young people and families."²⁹ In this context, it is interesting to note that Ofcom studies suggest that parents are more concerned about the media content delivered via the television (23% very or fairly concerned) than via a child's access to the internet (17%).³⁰

6. In his recent speech on Internet Safety the Prime Minister distinguished between two challenges: "the criminal and the cultural", namely, the proliferation and accessibility of child abuse images on the internet, and the fact that many children are viewing online pornography and other damaging material at a very early age.³¹ We agree with the Prime Minister that "...these challenges are very distinct and very different. In one we're talking about illegal material, the other is legal material that is being viewed by those who are underage." It is critical that these debates are left separate, and that discussion on the latter remains proportionate and balanced.

7. Arqiva believes that children and young people should be able to enjoy the benefits of digital technology and the internet, whilst having the right to be safe online. Indeed, the commitment to ensure child safety online is a matter of grave importance—and should be a shared responsibility between parents, businesses and the wider communications industry including ISPs, web publishers, WiFi providers and government. Therefore, Arqiva is pleased to be a member of the Internet Watch Foundation (IWF) and to have fully engaged with the UK Council for Child Internet Safety (UKCCIS), as well as government; key stakeholder organisations, businesses, retailers and manufacturers on this important issue.

Protecting Children through filters

8. As one of the six main public WiFi providers (with BT, Nomad, Sky, Virgin Media and O2), we provide internet access through WiFi, which is used by the public in a variety of means. Arqiva's recent contracts include the provision of WiFi to UK airports (including Heathrow; Stansted; Glasgow; Edinburgh; Manchester and Southampton); several hotels and retail environments (including Premier Inns and Enterprise Pubs); as well as several local authorities, including Manchester City Centre; and several London Boroughs.

9. As a member of the Internet Watch Foundation we are committed to blocking access to child sexual abuse content and other illegal material. We are also committed to blocking terrorist content, as well as intolerance and hate, and criminal activity. This applies across our network.

10. We believe that it is particularly important to have strong protection in public places particularly where unsupervised children might reasonably be found on a regular basis. Therefore, in the absence of a specific request from our business customers, we commit that our standard public WiFi offering will also include filters to block pornography. This will help prevent children and young people from accessing inappropriate pornographic material themselves, and should also limit accidental exposure to inappropriate material that nearby adults might be looking at in public.

11. Children gain access to the Internet from many devices: PCs, smartphones, tablets and games consoles; both their own and those owned by their friends and parents. Many of these devices gain access to the Internet via multiple networks: fixed broadband at home, mobile broadband and Public WiFi outside of the house. In simple terms, there are two main ways of filtering the Internet content presented to children:

- I. The network can filter content, for *all* users, or for children only, where the network can firmly identify the user and the age of that user.
- II. The device can be set to filter content, with device passwords to prevent children from changing these filter settings.

Arqiva believes that *both* measures are required to minimise the adult content available to children. The first would benefit from a consistent approach to content filtering for all Internet access networks that provide service in public places. The second requires education for parents and children, as well as a policy that all devices (and internet access software on those devices) should be supplied with adult content filtering turned on by default.

12. It is unfortunate that, on occasion, filters can also mistakenly "over-block" and prevent access to sites which parents would be content to let their children browse. Arqiva recognises this can sometimes be frustrating for consumers.

13. However, it is also important to guard against a false sense of security. Parents must be made aware that turning filters on does not immediately make the Internet "safe". Parents should be encouraged to talk to their children about what they do online and offline.

14. Filters can only block domains or websites—they cannot filter content or behaviour within sites such as social media platforms. Given that these platforms are a major driver of young people using the internet, it is important for these platforms to be vigilant themselves at combating cyber-bullying or anti-social behaviour.

²⁹ Do we have safer children in a digital world? A review of progress since the 2008 Byron Review—Professor Tanya Byron March 2010

³⁰ Ofcom's Children and Parents: Media use and attitudes report (Oct'12)

³¹ Speech by Rt Hon David Cameron MP, 22 July 2013—delivered to NSPCC

Protecting Consumers through education

15. Young people's use of the internet should be an incredibly rewarding experience—both within the school gates, and during their extra curricula home and social life. Activities that harness new technologies can make a valuable contribution to the wider school curriculum and to children's learning. Arqiva recommends that government place greater emphasis on internet safety themes across the educational curriculum. We believe that policy makers should do more to research and improve online protections for more vulnerable children; define inappropriate content and improve the means for identifying it online.

16. Arqiva are proud to work with government, UKCCIS and others to establish clear, simple benchmarks and classifications for parental control solutions. We believe parents should be empowered with the skills and knowledge to protect their children while going online at home. In particular, parental controls can help limit the chances of children being exposed to inappropriate online content. Arqiva welcomes parental control features that may be included in new technology such as personal computers, computer and video games, computer software, mobile phones and digital television services. These controls can be used to limit access to only age appropriate content, to set usage times and limits and to monitor activity.

17. There are many ways of accessing and downloading music, film, TV and video safely online and it is important that children and young people understand how to download content *legally*. Copyright law applies to downloading, sharing and streaming—just as in the world of physical CDs and DVDs. Improved “media literacy” should make explicit that those who make music, film or TV content available to others on a file-sharing network, download from an illegal site, or sell copies without the permission of those who own the copyright, are effectively breaking the law and could face serious penalties. In addition, illegal file-sharing programmes and websites pose greater risks to your computer or mobile phone than legitimate sites. Users often unwittingly download viruses or spyware and can inadvertently share personal computer files and information. Some files are purposely misnamed on file-sharing and peer-to-peer networks to trick people into downloading them.

18. When it comes to online safety, we also believe that media and communications companies, including the public service broadcasters, play a key role in educating the public. The BBC should be praised for regularly commissioning innovative, multi-platform content which inspires and educates audiences. The BBC's sixth Public Purpose includes “*Delivering to the public the benefit of emerging communications technologies and services:*” Indeed, the BBC's content and services are perhaps the most powerful means to drive adoption as well as to educate the public as to the risks of emerging technologies. The BBC is a trusted guide to the digital world for the inexperienced or unsure, a safe place to be for the young, a reliable and accurate on-air and online source for the information seeker, and a challenging and involving partner for the more advanced user. Ultimately, “online safety” should be regarded as an important plank of the BBC's commitment to support the media literacy of all its audience.

The need for research

19. There is a growth in using alternative portable devices (including mobiles and portable media players) to access online content in a variety of places and without parental supervision. Use of mobile phones continues to grow among young people—around 90% of young people over the age of 11 own a mobile phone. There is also a popular perception that online behaviour on shared devices in the family living room is “safer” than behaviour on mobiles, personal tablets or portable devices. However, Arqiva notes that some experts suggest there is little evidence on the links between using more portable devices and the online risks young people face in using such devices.³² Therefore, it is essential for policy makers and educators to continue to research and understand the many different ways that children and young people are using internet enabled devices, especially in the home and within social environments. Similarly, Ofcom has estimated that 43% of children have an active social network (Facebook, Myspace or Bebo) profile, and across social networking sites it is estimated that children aged 8–11 years have 92 friends—and have not met 12% of them face-to-face, and those aged 12–15 years have 286 friends—and have not met 25% of them face-to-face.³³ More research is needed to explore the links between where, with what, how often and with whom, children access the internet and the likelihood of online risks.

September 2013

³² NFER Report “Children's online risks and safety—a review of the available evidence” (2010)—commissioned by UKCCIS

³³ Ofcom's Children and Parents: Media use and attitudes report (Oct'12);

Written evidence submitted by James Griffiths

1. I am writing as a concerned parent and individual in relation to the current issue being considered by the Government relating to the safety of children from the corrupting content of adult material that can be viewed on the internet. I have seven children and along with my wife have sort to bring the children up in a safe and loving household while facing the everyday challenges of family life. This current threat is both disturbing and very harmful to the fundamental basics of family life and to the moral fibre of a right foundation for our young people.

2. We recognise that the internet has brought considerable benefits to both children and society in being used as a tool for gathering information especially in helping them with their studies. Our older children didn't have the same wealth of information when they were in education as our three younger siblings have now (aged 15, 13 and 11) but whilst we have blocks and filters in place ourselves there are many many other children who don't have this protection which leaves them very vulnerable to unsuitable and corrupting content.

3. We believe that much more needs to be done by the Government, industry, parents and young people to put in place measures to protect the youth of today and make the internet a safer place for children. It is a basic necessity that our children are safe from cruelty and harm wherever they are and that includes when they are on the internet.

4. When we talk about child safety online we believe two areas of greatest concern and areas that need to be focused on are:

- Keeping children safe from harmful content online (eg grooming and sexting).
- Protecting young eyes from legal content that's not appropriate for their age.

5. It is not a new issue facing the Government as many persons and organisations have been calling for years for policy changes and investment of resources in both technology and policing to better protect children and young people from online dangers

6. Along with many other concerned parents we are calling on the Government and especially this Committee with its responsibilities in this particular matter to bring in legislation that would require default blocking of all adult content to be a standard setting on all internet enabled devices sold in the UK. This would a way of stopping children from seeing harmful adult content and give peace of mind to parents when the internet is being used. There is also a need of the development and use of better age-verification software.

7. The constant attempt to water down this action being taken in the name of freedom of choice is a very poor argument indeed and surely recent statistics from Ofcom revealing two key facts—"81% of children aged 14–16 have viewed **ADULT** material online" and "Only 46% of parents have filters in place on their home internet"—only serve to illustrate the urgent need of action as to this very serious issue.

8. My wife joins with me in my grave concerns as to this matter and we would urge you as a committee to take account of these concerns along with many other parents like ourselves in moving forward to implement the necessary actions to give our very treasured possessions and the hope of the future in this country—**our young impressionable children**—the protection and moral support they need to prosper.

September 2013

Written evidence submitted by Christopher G. H. Thomas

- I wish to make a submission to the Committee as an individual, a parent and grandparent, a practising Christian and as a user of the internet.
- I understand the great advance that the internet has brought to young people in accessing the immense wealth of information available to assist them in their studies and other areas of normal life.
- However, it has unquestionably brought with it very great moral dangers and much material which damages children and adolescents. Included with this is access to images and information which is inappropriate for those in developing years. They are just not able to handle such things at that age.
- I recognise that parents have a major responsibility to protect their children from contact with damaging or corrupting matter on the internet, but would respectfully submit to the Committee that the Government also has the responsibility to use its power to provide suitable protection.
- Measures I would submit to the Committee as things the Government should do are:

1. Make it a legal requirement that all internet-accessible equipment and devices sold in the UK have a default setting as standard that all adult material is blocked.

2. Software to verify the age of users should be improved, and the Government should promote its use strongly.

3. The Government should use its authority and influence with manufacturers to ensure that they put into practice such measures. They should not be diverted by suggestions that they are impinging on individual freedom.

THE PRESERVATION OF BRITISH YOUTH IS AT STAKE IN THIS MATTER.

September 2013

Written evidence submitted by John Edgar Cameron Lowe

ONLINE SAFETY OF CHILDREN

Thank you for this enquiry and allowing some of us to make a submission.

I write in a personal capacity as one who, with my wife, have constant contact with children through the church.

Sex is a very powerful force in many people's lives.

When in its proper setting of raising children it is a good and right thing.

When out of its setting it is like fire out of control and does damage.

I have personally been damaged by adult material although this was in an age before the advent of the internet. I have felt the effects of this damage throughout the rest of my life.

Today the chances of children being damaged are enormous compared to years ago. I therefore fully agree with David Cameron, Michael Gove and others, that every possible effort should be made to get government, parents, internet providers, educators and charities to work together to provide all the protections necessary to safeguard them from the many different types of sexual corruption available online.

It is surely a crime to shatter the innocence of children and young people.

There is a solemn piece on the last page of the Bible that speaks of those that love and make a lie.

Those that *make* a lie are those that set up and publish these damaging and vile things.

Those that *love* a lie are those that delve into and watch them.

As responsible citizens, as many as possible need to do everything they can to address this massive problem.

May you all be helped in your deliberations.

September 2013

Written evidence submitted by Norfolk Library and Information Service

SUMMARY

- Internet access is possible in a range of environments—a one size filtering solution will not fit them all.
- Most library services already have internet filtering mechanisms in place.
- National standard needed to determine what type of information is acceptable in age bands—schools, parents, internet industry and filtering software providers will all need to sign up to it.
- Standards will need to apply to volunteer run libraries, who may not have the necessary expertise.

EVIDENCE

1. There are a number of possible environments where children can access information online:

- Home.
- School.
- Library Computer or authenticated library wifi access.
- Internet café.
- Open access public wifi hotspot (including in libraries).
- Authenticated access public wifi hotspot.

Any recommendations will need to reflect on the conditions that apply in each environment—not all conclusions can or should necessarily be applicable in all environments.

2. Further comments will be restricted to internet access in libraries.

3. Library services should be able to identify who is logging onto a public computer or authenticating onto their library wifi access. In Norfolk this is achieved through the use of a borrower number and PIN combination. This means that it should be possible to require library customers to agree to abide by an Acceptable Use Policy, which among other things would include agreement not to access sites or material that is “is obscene, racist, defamatory or otherwise unlawful, or that would cause harassment or gross offence to others”.

4. It is then possible to withdraw internet access privileges if this agreement is breached.

5. To prevent breaches, most library services subscribe to an internet filtering service, which is configured to prevent access to sites falling into a range of categories. In Norfolk, this is the same product that is used for filtering staff internet access, so any product must be capable of handling more than one filtering regime profile.

6. We use the same filtering product for our public wifi access in libraries as we do on static computers, although we believe this is by no means a common feature in other library authorities.

7. Different filtering products categorise sites differently, so application of a national standard will be difficult—filtering service providers regard their classification methodologies as commercially confidential.

8. Filtering is applied at the site level, not at the content level. It is therefore not currently possible to block adult video content on YouTube without blocking all video content.

9. YouTube is the default hosting service for all Norfolk County Council public video content, so any idea of a national block on providing access to YouTube in libraries would have significant impact on the delivery and distribution of information about council services.

10. Norfolk Library and Information Services would like to see all websites that do or may host adult material to be required to hold it in an easily identifiable section of their site, so filtering software rules can be applied.

Norfolk Library and Information Service do not currently make any distinction about what a customer can access, within the bounds of our acceptable use policy, based on age.

This is largely because there is no national standard about what is and isn't acceptable within each age range, or even what those age ranges should be.

Our current age categories for borrowing books are:

Under 5
5–11
12–15
16–18
Over 18

11. Norfolk Library and Information Service does not view it as the responsibility of a local library service to determine what is acceptable at each age, nor do we have the resources to do so—that should be set nationally and applied consistently across all filtering services so no local variation is possible.

12. Norfolk Library and Information Service does currently view it as the responsibility of the parent or guardian to monitor and control the internet activity of their children while they are on library premises. Our safeguarding policy states that no children under the age of 8 should be in a library unaccompanied.

13. Having said that, use of computers in libraries in Norfolk by children and young people is not that high, according to our usage statistics. However, as more free public wifi is rolled out across Norfolk, we may find the proportion of children accessing the internet across our wifi network (and hence our filtering regime) but on their own devices increases.

14. Access to social media sites is one of the most popular uses of public computers and is used by customers to keep in touch with their friends and family across the world. Any recommendation to filter out use of social media sites in public libraries would have a severe impact on the positive benefits of social networking for library customers. For this reason we would be opposed to the principle of blocking internet access to social media sites in libraries.

15. Management of a filtered internet service requires resources and a degree of technical expertise to provide it. This is a skill set that will probably be unavailable to most groups who may wish to take over the running of a local library service on a voluntary basis.

There should therefore be a commitment that the local authority will make sufficient funding available to continue to provide a comprehensive and secure IT infrastructure in volunteer run libraries. This will also help to support the Government's Digital by Default policy.

Written evidence submitted by Phil Alexander

Children nowadays have the ability to access large quantities of very useful information effectively replacing the large and space-taking encyclopaedias of days passing.

What ruins the good that we appreciate is the low down, corrupting content that even adults are safer without.

As a parent of four children I would welcome a large padlock on all content that was unsuitable to children, the key to which would also be locked away.

Please could the Government urgently develop a secure firewall and legislate a mandatory download that blocked such content and the owners of computers that feel they must defile themselves, would have to apply to a Government watchdog?

Why do less than half of our parents have blocks on home computers? If the parents aren't bothered, pity help the children.

I appeal to the pity there is in the House, to have the heart to get this cracked.

September 2013

Written evidence submitted by Ben Hardwick

I am delighted to hear of your committee's laudable efforts to look into the subject of the damage that can be done to the younger generation by uncontrolled internet access—thank you very much for launching this enquiry.

The ordered, peaceful and generally prosperous outward-looking UK society with its opportunities, comprehensively organised education, healthcare, aid, infrastructure and defence/security arrangements are a priceless result of the daily work of Government—something that is rarely recognised or valued like it should be.

These benefits also extend far beyond Britain's shores and the UK is still a beacon of tolerance and crucial lynchpin of global peace and security as well as being an example that is frequently followed by other Governments and States.

Little wonder then that Government is undoubtedly an instrument of God—1st Epistle of Peter, Chapter 2, V13; it is a “giver” and “provider” as well as a “controller”—again, the Bible states in the Epistle to the Romans Chapter 13 “for he bears not the sword in vain” along with a good deal else.

Government's first duty is the protection of its citizens—this is an area at which HMG excels whether in defence and intelligence matters or law-enforcement that stabilises and enhances the condition and experience of society and its citizens and the whole global community.

I seek by these few paragraphs to set out simply how absolutely right it is for you to persist with better control measures on internet viewing and that you may be encouraged and set forward in doing what is clearly your duty.

I am a father of four children from three to 10 years old and revel in watching their rapid development and willingness to absorb knowledge at an apparently impossible rate. They are very impressionable and it is a very great responsibility as parents that my wife and I have in protecting and nurturing the next generation into responsible citizens.

Affectionate control and unselfishness is absolutely critical in this and it is really tragic to hear figures from OFCOM that more than 75% of 14–16 year olds have accessed adult material.

This is a situation that will cause permanent mind-scarring and a lack of fidelity and stable relationships on which true happiness is built in our society—to say nothing of the cost to Government and the taxpayer of broken homes because of so-called freedom to look at this content when in one's tender teens.

HMG should move forward fearlessly with comprehensive and efficient control measures of what is currently a lawless “wild west” of media so as not to fail the potential of following generations.

It is a most revolting and immoral thought that there are actually publishers and persons making millions out of degrading us and ruining the moral compass of the young in our society.

I believe that there should be default blocking of all adult material on internet enabled devices sold in the UK as soon as possible.

I wish you all the best and courage in your deliberations on this vital subject.

September 2013

Written evidence submitted by John R. Edwards

SUMMARY

- The present position of unlimited access to online material is morally dangerous and requires control;
- Some form of censorship should be established to determine what should be classified as “Adult Material”;
- Parameters should be established as to what classifications of material should be eliminated from online availability;
- Grades should be established to determine what material is acceptable for access by young people;
- Age levels should be established to determine when access should be allowed to “Adult Material”;
- Controls should be instituted which bar young people from access to material deemed unsuitable for them;

SUBMISSION

1. The Inquiry into this subject arises from the fact that, at the present time, there is no restriction placed on the Internet in respect of juvenile access to material widely accepted as unsuitable for them. Furthermore, such online material is not graded and in the eyes of many much of it is regarded as being in the nature of cruel, salacious and/or obscene. Some would go so far as to say that at least some of it is potentially harmful even to adult viewers.

2. Concern has been increasingly evident that action is required to ensure that some kind of control is established that will at least protect young people in particular from access to material regarded and classified as “Adult Material”.

3. As a lifelong committed and practicing Christian, and as a parent, grandparent and great-grandparent of a total of just on 50 children, grandchildren and great-grandchildren, I have an intense interest in the moral safety of young people and am concerned to witness to the Committee my views, with which many would, I am sure, join, that action is urgently required to bring in a measure of protection for young people against the existing access to the volume of unsuitable online material that is currently so freely available to them.

4. Children are the potential for the oncoming generation. We need to be thinking and planning now for the wellbeing of that new generation. If we permit freedom of access to and do not control the supply to our children of, morally damaging material, the next generation will, inevitably, be basically corrupt. If we are planning and endeavouring to ensure a well educated, law-abiding, honest, principled and upright next generation, we must act now to make as certain as we reasonably can that they are morally equipped to be convinced of and to maintain an upright way of life and to suitably educate *their* next generation. If, on the other hand, we allow the standard of life to drift whichever way it may go, the result in the oncoming generation could be intolerable, bordering on anarchy. The fact is that people are only law-abiding because they are taught so to be. If the reins of law become slack, the quality of life deteriorates to the point where people do what is best in their own interests regardless of the effect it may have on others.

5. Consideration needs to be given to the ambitions and character that should characterize the oncoming generation. Parental influence needs to be promoted and parental responsibility encouraged so that they teach their children the basic principles of an acceptable way of life.

6. Sex education, whilst theoretically justifiable, inevitably stimulates many children to enquire into what, in effect, is pornography. The basic thinking behind the conception of sex education is clearly the concern that children need to understand the inherent dangers that ignorance involves. Whilst this train of thought is understandable, the real responsibility as to sex education devolves on the parents and the fact that the responsibility has been included in the state education system is an acceptance of and pointer to the fact that parents have been neglecting their duty in this regard.

7. The onset of the IT age has resulted in the computer becoming an essential to life. Children become addicted to the machine to the point where they may feel compelled to use it even to do simple calculations that in times past would have been regarded as mental arithmetic. It has become an avenue for exploration and inevitably children use it to satisfy curiosity in various avenues, many of which are very beneficial. As a tool for subject research it can clearly be advantageous and valuable. Regrettably, however, the freedom of access and the almost infinite range of material available currently enable children to attempt to satisfy their innate curiosity by gaining access to material that could be morally damaging. This is clearly the concern of the Inquiry.

8. The United Kingdom has established and maintained a rule of law based on democracy and the freedom of speech. As political views have changed and the availability of information has increased and become more widespread, it has become increasingly necessary to ensure that established media standards are maintained. This has been generally accepted by the population and political parties have, in the main, worked together to ensure the maintenance of the principles governing media standards.

9. In current law regarding media, there are clear standards concerning what may and what may not be published in newspapers, journal and films. On the other hand, the development of the internet has resulted in

a virtually uncontrolled flow of material, quite an assortment of which would not be permitted in a newspaper or journal. What is even worse is that there is no control on the access to such material, whether by adults or children. It is indeed questionable whether such cruel, salacious and/or obscene material, which could not legally be published in a newspaper, should be available at all, whether to adults or children, on the internet.

10. Children generally learn the benefits of access to the internet without necessarily being taught any form of control, leaving it to their judgment as to the limits that they should apply to their access to such material. Indeed, such is the availability of material, that, in the absence of control, it is incredibly simple, once one learns the method of access, for them to gain entry to such sites and to spend as much time as they wish in digesting the stuff.

11. Voluntary controls are available. Thoughtful parents, concerned with the upbringing of their children, can install filters on their computers that limit the availability of access. We are told that 46% of parents have taken advantage of such methods of control and they are to be commended for their action, but that leaves 54% that have not done so, and whose children are therefore vulnerable to the range of such unsuitable material that is so simple to access. Indeed, we are told that 81% of children aged 14 to 16 years have viewed what would be regarded as “Adult Material” online—a very worrying fact.

12. The current law in this country grades films for public showing according to the composition of the audience, in an endeavour to protect young people. The concern behind this Submission would be as to whether it would be possible to apply that principle to the internet. In presenting this Submission, the concern is to underline that the present position is morally unacceptable, to determine what controls need to be established in order to bring about essential control and to encourage the institution of the necessary legislation as quickly as is reasonably possible. The present position is serious and needs urgent attention. The present Inquiry is valuable and places a huge responsibility on the members of the Committee. The concern is to support the Inquiry and those who are appointed by drawing attention to how the present position is regarded by persons who have for a long time carried a serious concern as to the subject.

13. When such legislation is prepared for Parliamentary consideration and enquiry, it is inevitable that some persons and organizations will complain that people’s freedom of expression is being limited. The present law as to libel, slander and sedition already puts certain limitations on the freedom of expression and what is being considered is not incompatible with that. The recommendation would be that the present legal framework should be extended to cover and include such matters as corrupting views, not only sexually explicit words and pictures, but also violence, cruelty and the promotion of terrorism.

14. I submit therefore:

- (a) That the present position of the unlimited access of young people to online material is morally dangerous and requires a reasonable level of control;
- (b) That some form of censorship should be established that reviews material available online with a view to determining what material should be classified as “Adult Material” (and therefore limited to viewing by adults) and what should be freely available;
- (c) That the consideration of (b) above should extend to the setting of parameters as to what may be published on the internet and to establish the necessary legal framework to ensure that certain types of explicit sexual material and of violent, cruel, terrorist-promoting and obscene literature should be eliminated from the internet;
- (d) That, as a result of (b), grade levels should be established that determine what is acceptable and what is not acceptable for access by young people, in respect of such material;
- (e) That age levels should be established, probably in line with film viewing levels, that will determine at what age young people may access such material;
- (f) That controls should be established which bar young people from online access to material deemed dangerous for their consumption.

September 2013

Written evidence submitted by Chris Evershed

Our young people are the future of the nation. Without them there is no future. How careful we need then to be in caring for and educating them so that a generation emerges that the country can be proud of.

The internet has brought considerable benefits to children, society and the business world. However it can, and is, being used to corrupt society and the very children that it should benefit. It is a sorrowful statistic as stated by Ofcom, that 81% of children aged 14 to 16 have viewed adult material online, whilst only 46% of parents have filters in place on their home internet.

Pornographic images can be viewed on the internet by young persons, so warping their minds. This can only lead to a rapid decline in moral standards, increased delinquency, dysfunctional families, and a proliferation of adults with no moral structure or ability to discriminate between right and wrong, good and evil. Because they see adults engaging in such actions it must be OK.

The government needs to act now and decisively, to address this extremely serious problem. Default blocking of all adult content should be the standard setting on all equipment sold in the UK that is able to access the internet, combined with robust age verification. Without this, children will continue to be damaged irretrievably.

There is also a tremendous increase in child pornography polluting the internet, and research by the Child Exploitation and Online Protection Centre (CEOP) has alleged that more than half of those who view child abuse images go on to commit abuse themselves. This is a proof of the vicious spiral of moral decline that sets in when such activity is allowed. Internet Search Providers should be held responsible to track down child pornography and remove such images from the internet.

It is well to remember that the decline and fall of the Roman Empire was not due to any lack in the military might, by which their empire was formed, but by moral decline and degeneracy.

September 2013

Written evidence submitted by EE

INTRODUCTION

1. EE welcomes the opportunity to provide comments to the Culture, Media and Sports Committee inquiry into Online Safety.

2. We treat this issue with the utmost seriousness and we recognise that, as the ways in which we all get connected to the internet develop, we have a responsibility to ensure a safe experience for our customers and for their children. This is a challenge which will continue indefinitely as online safety and the control of harmful content requires unrelenting effort by individual companies, as well as collective endeavour.

3. EE is a British company which provides service to 27 million customers on EE, T-Mobile and Orange plans. In addition to voice and text, we host a variety of content services including music, games and video clips which are available within our mobile portals (Orange World, Web n' Walk and T-Mobile) as well as providing general internet access. We also run a fixed ISP (EE Home) which currently has around 750,000 customers and a corporate WiFi service.

4. Turning to the particular issues raised by the Committee, this paper comments on the best approach to protecting children from accessing inappropriate content, recognises that technical solutions are only part of the solution and that education for children and parents is key and that both network and software filtering can meet the requirements of family friendly and effective filtering. It then details EE's own policies on e-safety and addresses the issue of blocking other harmful content.

HOW BEST TO PROTECT MINORS FROM ACCESSING ADULT CONTENT

5. EE strongly believes that the best way to protect children from accessing inappropriate content is by a combination of parental controls and education. Blocking websites maybe sufficient protection for a young child but will not deal with the needs of young teenagers who will use social media and other personal communications. Teenagers in particular will always try and find material that their parents or teachers would rather they did not see, and it's the industry's role to provide educational material, as well as the tools, to ensure children and parents are well equipped to make informed choices and do not inadvertently come across material that is not appropriate for them.

PARENTAL CONTROLS

6. EE supports the recommendation that came out of the Byron review of "active choice" or "unavoidable choice" where parents are forced to make a decision on whether they wish to apply a filter, as opposed to an across the board "default on". The principles of "unavoidable choice" as set out in the Government's white paper "Connectivity, Content and Consumers" include the availability of family friendly filters that block adult content for both new and existing customers, the need for customers to make a choice about whether they want filtering at first connection to the internet or at point of sale, age verification of the person setting up or removing the filter and communication of the benefits of filtering. These principles can all be met through either network based filtering or software based filtering on devices.

7. There is no "one" right answer for all customers, across all platforms or all devices. EE supports an approach that allows for a portfolio of network based and device based solutions to meet the needs of the tens of millions of people in the UK that access the Internet, through PCs, mobile devices, games consoles and, increasingly, TVs.

8. There are very good reasons why mobile and fixed operators have chosen to take different approaches to the delivery of parental controls for mobile and home internet. On mobile phones operators filter adult content on the network and it is on by default for all customers and can only be lifted on proof of age. On the fixed home internet many ISPs offer all customers free parental controls and provide unavoidable choice on set up. This difference of approach is because the way people purchase mobile and home internet differs:

- all home internet customers sign a contract and are adults;

- the home is likely to contain a number of PCs for each family member, each requiring different levels of filtering, and some no filtering at all; and
- households attempting to accommodate this mix of PCs via a *single network filtering profile* are likely to experience dissatisfaction, and may well turn off filtering altogether. Allowing different PCs to be protected via their own filtering software provides the necessary degree of flexibility.

9. For mobile phones we filter content at a network level and it is set as on by default. This is because:

- Mobile phones unlike home computers are personal devices and so a single filtering profile is effective.
- Filtering software is not available for all mobile devices. Different operating systems (Android, Apple, RIM) each require a different solution which is why operators implemented a network based approach.
- Mobiles are often bought by children who are unlikely to request at point of sale that parental controls software should be activated.
- Many mobiles are sold through independent retailers where operators have little or no control over how the devices are sold or who they are sold to. The purchasing decision for mobile is very different for fixed with many indirect channels of distribution (such as supermarkets) who are not set up to discuss the benefits of parental controls.

10. Given that the majority of children are highly technically proficient and routinely share tips and information, it is considered that such controls would offer little or no practical protection. We continue to evaluate options for offering greater controls on mobile devices and will revisit this if viable solutions are identified.

11. As we have explained there are good reasons for taking different approaches for filtering mobile and fixed traffic. In addition, we believe mandating network filters for all fixed ISPs in order to have filters which are on by default, will be a huge expense and take considerable time to implement. The initial investment of providing network filters on the mobile network costs millions of pounds and there are also ongoing costs for maintenance and for the categorisation and filtering suppliers.

12. More information on the parental controls available across EE's mobile brands, fixed business and Wifi network is set out in Appendix I.

EDUCATION AND ADVICE

13. Parental education and engagement is vital. As Dr Tanya Byron set out in her review on child safety, parents have a responsibility to understand what their children are viewing and to educate themselves and their children on how to assess the appropriateness of content.

14. Education is so important particularly for teenagers and older children who want more choice in what they are able to access. Since access controls were put in place, content on the internet has continued to develop and more players are involved in its delivery. This means that even with the best filters available it is increasingly hard to block inappropriate content particularly on social networking, interactive sites and app stores. Raising awareness of e-safety through diverse channels therefore remains of paramount importance.

15. Our research shows that parents often feel overwhelmed and unable to keep up with the pace of change and consequently what their children are doing online.

16. Parents need to be made aware of the risks and given clear, simple signposting to sources of information and tools to help them manage their children's online life. This would include clear messages about what the risks are and tools such as help with setting up parental controls.

17. We also advocate a "talk & trust" approach whereby parents are given guidance on how to open up dialogue and have conversations with their kids so that they understand the risks. We don't believe that blocking and banning on every level is a sustainable solution as children will always rebel and find new ways to express themselves. It is far more important to arm them with confidence and trust and provide them with information to help them manage the risks as well as their parents.

18. As part of our rebranding, we recently updated our online safety information and launched EE's Digital Living website with dedicated pages on keeping families safe online. <http://explore.ee.co.uk/digital-living/keeping-children-safe>

19. This includes a series of six short films together with activity guides, so parents can talk about e-safety issues with their children. The films cover a variety of issues including cyberbullying, digital footprint and posting information online and are EE branded versions of films provided in our previous award winning Orange education programme which had reached 67% secondary school penetration by the end of 2012.

20. Our network of employee volunteers (e-Safety Champions) reached over 10,000 young people directly with e-safety messages from 2009–12 as part of an employee engagement programme.

21. We continue to keep our material up to date and have recently updated our advice for parents leaflet which provides guidance on a range of issues including setting parental controls, cyberbullying, sexting, privacy settings, social networking, downloading illegal copyright, how to report abuse and controlling costs. The leaflet "Advice for parents" is now in all 600 plus EE stores nationwide and is also available from our Digital Living website.

22. By the end of the year all our frontline employees in retail and customer services will receive online training on E-Safety and Active Choice highlighting the tools and materials on offer across the brands. This module will also be included for new employees within their induction training.

PROMOTING ONLINE SAFETY IN SCHOOLS

23. In EE's opinion more emphasis is needed in PSHE as part of the curriculum and specific attention given to e-safety issues. We feel that as a network operator we have a duty of care to provide information and guidance on how to use our technology in a safe and responsible way. We can share these messages with existing and new customers and our free education programme which is used in 67% of secondary schools shows that we go beyond this and out into the community. However the education system plays a vital role in equipping young people with life skills. With less emphasis on PSHE in recent years we feel the issues are not getting the traction they need. It should not be solely up to the network providers to fill this gap but rather for the education system to embrace the materials and resources that our organisations can offer and build them into daily school life. EE will continue to develop new materials on e-safety in the future for our website, but the real key to success is the way these, and other organisations' resources can be slotted into a relevant and robust curriculum, so that teachers can take advantage of them.

CONSISTENT APPLICATION OF ACTIVE CHOICE

24. ISPs no longer control all aspects in the value chain. We firmly believe that content providers and increasingly device manufacturers have a significant part to play in child safety if controls are to remain effective. Government should also be ensuring that the responsibility for child protection applies across the wider value chain with manufacturers, software providers, WiFi providers, search providers and social networks, as well as ISPs. Not only will this provide more channels to market for child safety messages and products but it will also ensure there is a level playing field in terms of implementation costs and responsibility.

25. Furthermore WiFi providers and manufacturers of consumer electronics products such as games consoles, smart TVs and set top boxes, which are offering an ever richer and open online experience, should also be required to offer active choice.

FILTERING OUT EXTREMIST MATERIAL

Tackling Child Abuse Images and the IWF

26. EE has been an active member of the IWF for nine years and is one of the companies that contributes the maximum amount to the IWF. We fully support the recent extension to the IWF's remit to allow proactive reporting by the IWF (rather than only investigating reports made through the hotline). This will lead to a more effective use of the IWF's resources. Any subsequent proposals put forward by the IWF should always be supported by detailed plans and agreed through the normal budgeting process.

27. EE has never received a notice to take down content for any of our hosted services. We have strict guidelines on the type of content hosted on our mobile portals and our interactive services such as chatrooms, message boards and commenting facilities are all moderated.

28. We implement the IWF's child abuse blocking list across all our platforms each day and return a splash page to those customers looking for or stumbling upon illegal images. We also participate in the quarterly testing programme to confirm that the block is operational.

BLOCKING OTHER FORMS OF CONTENT

29. There have been increasing calls by Parliament and lobbying groups for other types of illegal or inappropriate content such as extreme pornography, racist or anorexia sites to be subject to the same treatment as child abuse images with ISPs blocking offending websites for all its customers. For EE there are practical and policy concerns with extending full blocking into other areas. The challenge comes in areas where there is no consensus on the appropriate role of providers. Asking ISPs to block content that is offensive to some people but is clearly legal, places ISPs as arbiters in deciding what customers can access.

30. We believe it is ultimately for Parliament, not ISPs, to take a view on unpalatable content and to determine what is illegal or whether the legislative framework requires revision. The current process with online copyright is that the courts through a court order decides whether a website is facilitating access to illegal material and which IP addresses should be blocked and on what terms.

RADICALISATION/TERRORISM

31. EE believes that sites that promote radicalisation and terror sites (as defined in the Terrorism Act 2006) are already filtered by our mobile parental controls under the “criminal skills” or “hate” or “violence categories”. However to be certain we require the Home Office to send across a list of the websites so we can check how they are categorised by our filtering supplier.

PREVENTING ABUSIVE OR THREATENING COMMENTS ON SOCIAL MEDIA

Social Media

32. Social media and interactive services have revolutionised the way people connect with each other and offers tremendous benefits. However EE recognises there are concerns over potential access to inappropriate content, bullying and grooming. Due to the sheer volume of postings moderation of all content is impossible. However providers could publicly commit to respond to all reports of potential child abuse, grooming and bullying with an agreed time (such as 48 hours). Furthermore greater transparency of the safeguards available on sites should be available as these vary greatly between services. We also believe that some moderation of content that has potentially the most harm could be implemented.

33. All user generated content that EE hosts on our portals (T-Zones, Web n’ Walk and Orange World) including chatrooms, video sharing, picture galleries, message boards and commenting services are moderated by trained staff working to a documented and defined set of standards that define who is able to use the service and what constitutes acceptable behaviour. There are slightly different policies in place for different services and between the brands however all images are pre vetted against agreed guidelines before they are posted online. In addition we have clear policies on dealing with complaints and on notice and take down.

34. Our message boards are moderated by EE Digital Staff and we also have a Site Feedback form where people can contact the editorial staff to flag any issues. This is monitored between 9am -5pm every day of the week. If there is an instance where we need to take down content that is already live we aim to do it in less than 30 minutes. However the frequency of complaints is very low.

35. For article commenting we enable customers (or anyone who is viewing the website) to report abuse. This is sent to a live dashboard which our moderation company monitor.

CYBERBULLYING

36. EE’s Customer Services provide advice to customers who are concerned about bullying by text or on calls. If the problem persists customer services can offer to change the customer’s phone number and the most serious incidents are referred to the Nuisance Call Bureaus where dedicated staff help customers who wish to report cases of harassment or malicious calls to the police. The Nuisance call bureaus receive around 300 enquiries per month and of these around 50 will be referred onto the police and the remaining 250 will be provided with appropriate advice and guidance.

APPENDIX I

EE’S PARENTAL CONTROLS

PARENTAL CONTROLS—MOBILE

All three mobile brands (EE, Orange and T-Mobile) offer the highest level of protection:

- All prepay and contract customers are offered parental controls free of charge and this is applied **by default** for new customers across **all** mobile devices (handsets, dongles and tablets). Age verification (via credit card, name and address check or instore) is required to lift the controls.
- All networks now offer **three** parental control settings: Strict, Moderate and Off. We are the only mobile networks to offer a Strict setting as we recognise that parents of younger children may want to filter some content which is not classified as “18” but that they don’t wish their children to view.

The three settings manage visual content (both commercial content and websites) as follows:

- **Moderate**—this is the default setting which will be on for all customers. It allows customers to view user generated content but blocks “18” content as defined by the BBFC (British Board of Film Classification) based on the BBFC’s Classification Guidelines which are the result of public consultations held every four to five years. This is wider than pornography and also includes criminal skills, drugs, gore, hacking, hate, self harm, suicide and violence. For more information see <http://www.bbfc.co.uk/what-classification/mobile-content>
- **Strict**—on request customers can select this setting which blocks all “18” content as above plus content that is deemed unacceptable for younger children including dating, cyberbullying, unmoderated user generated content, chat, glamour, occult, weapons and cults.

-
- **Off**—on proof of age (such as credit card or name and address check) customers can switch off filtering which gives access to the open internet. The Internet Watch Foundation list is still filtered for all customers.

EE has invested, and will continue to spend, millions of pounds in setting up and operating our parental control systems offering the best solutions that are available to the industry. The current filtering arrangements have been in place for nine years and work well with very few complaints about children viewing 18 classified content on their mobile devices. Customers who believe content or websites have been misclassified can email safeguard@ee.co.uk. This email box is forwarded to the Safeguard Product Manager and issues are dealt with within 48 hours.

Our Digital Living website provides detailed information on our parental controls, the full list of the categories blocked for each setting and how to report abuse or misclassified content <http://explore.ee.co.uk/digital-living/keeping-children-safe>

PARENTAL CONTROLS—FIXED

EE Home (our fixed business) now offers all new and existing broadband customers McAfee Family Protection software which is free of charge for 12 months. Customers can install the software on up to five devices are protected even when they're outside the home as the software sits on the computer.

It offers five predefined age settings (under 5, 6–8, 9–12, 13–15 and 16–18) and parents can also customise the settings, add or delete websites and set time restrictions. It also provides activity reports detailing web activity and it will send email or text alerts if access to inappropriate websites is attempted. It will also report on what information is being shared on social media sites and by instant messaging and blocks the downloading of music with explicit lyrics. The software is easy to install and we have developed a help video with McAfee which is available on our safety website.

We actively promote parental controls at point of sale and at all points in the customer's journey including in the Welcome Pack, in the router guide, in the customer's first email after activation, in the Home Mover Pack and Online on our Digital Living Website. Twice a year, as part of the EE Broadband Newsletter, we include information on the Family Protection Software to existing customers. We will also send a dedicated email to all customers every six months highlighting the benefits of online security and parental controls.

By the end of the year all new broadband customers will be presented with a "splash page" when they open their browser for the first time which will force them to make a choice on whether to download the parental controls software. If they choose to opt for parental controls they just click on the link provided which will take them straight to the McAfee download page.

PARENTAL CONTROLS—WIFI

EE offers both branded and white labelled Wi-Fi services to a range of corporate customers. We are engaged in the UKCCIS (UK Child Safety Council) working group and we are committed to offering a Family Friendly Wi-Fi service. All our hotspots currently block illegal child abuse images on the IWF list. By the end of the year we plan to set Adult Content filtering as "on" by default. It is then up to the venue owners to actively choose to disapply the filter if they want to.

September 2013

Written evidence submitted by BCS, The Chartered Institute for IT

The Institute promotes wider social and economic progress through the advancement of information technology science and practice. We bring together industry, academics, practitioners and government to share knowledge, promote new thinking, inform the design of new curricula, shape public policy and inform the public.

As the professional membership and accreditation body for IT, we serve over 70,000 members including practitioners, businesses, academics and students, in the UK and internationally. We deliver a range of professional development tools for practitioners and employees.

A leading IT qualification body, we offer a range of widely recognised professional and end-user qualifications.

www.bcs.org

HEADLINE POINTS

- The public, both collectively and individually, hold conflicting views on the balance between privacy and protection;
- It is impossible to prevent knowledgeable determined people accessing material, however "illegal", if that material is anywhere on the Internet;

- However, it is possible to make it less likely for naïve users to stumble across material that some agency (which? and how?) has deemed to be offensive;
- The question of what is offensive is one that calls for human judgement, is often context-dependent and that human judgement may be highly controversial;
- Individual cases prompt knee-jerk reactions, but “hard cases make bad law”;
- Preventing someone accessing something that they regard as desirable is likely to encourage them to adopt evasion technologies, which nullify *all* filters, not just those for material thought undesirable.

BACKGROUND

1. In order to access a document/film/video across the internet one has first to know where it is (discovery) and then have its data on one's device (delivery). Delivery is the business of Internet Service Providers (ISPs), while discovery is generally the business of search engines, but also of catalogues, such as Facebook links, recommendations, word of mouth and rumour in school playgrounds.

2. The Internet Service Providers are doing business in this country, and know who their customers are (in the sense of who is paying their bills). They are subject to various forms of UK regulation and legislation. The search engines may or may not be based in the UK. They may or may not have any office or business in the country and may not be subject to legal or moral pressure by the UK authorities. The Prime Minister's speech was somewhat confused when he said; *“the search engine shouldn't be involved in finding out where these images are because the search engines are just the pipe that delivers the images, and that holding them responsible would be a bit like holding the Post Office responsible for sending illegal objects in anonymous packages”*—the ISPs are the analogue of the Post Office, not the search engines.

3. It is important to understand that all documents (such as films and videos) are delivered across the internet as if they were live broadcasts: no intermediary holds the entire document for analysis. A good analogy is that of a service reading books aloud. There are then two fundamentally different approaches to censorship (which is the main issue).

4. One is **black-listing**: analogous to *“I'm not going to read you that book because it's called 'Lady Chatterley's Lover', and I've been told not to read that book”* or *“I'm not going to show you that film because it's classified 18”*. The major problem with this approach is that a vanishingly small proportion of the internet has been examined for banning/classification.

5. The other is **content-based filtering**: analogous to *“I'm going to stop reading that book now because I've come across this banned word in it”*, or *“I'm going to stop showing this film because the last frame was more than 40% 'pink' (sexualised imagery)”*. There are two problems with this approach. The first is that, under the Regulation of Investigatory Powers Act, it is probably illegal for ISPs to do. The second is that of false positives: many books contain occasional “banned” words, and a frame may well be “pink” because of a sunset, or a swimming gala.

6. The same objections apply to hybrid approaches, such as *“I'm going to stop reading that book now because I've come across a mention of a gamekeeper called Mellors”*.

7. These difficulties should not be minimised. It would be no defence under the Regulation of Investigatory Powers Act for an ISP to argue that the consumer (typically the parent of the child actually using the connection) has consented: *both* participants to the connection have to consent to the interception, and it is hard to see how an automatic web-server can consent.

8. Equally, the Chinese had a significant research project as part of what is generally termed “the Great Firewall of China” to search for “inappropriate” skin tones, but that project has apparently been abandoned.

9. A further problem is that what is “abhorrent”, or even “illegal images of children”, is context-sensitive. It is easy to say “medical textbooks are a special case, and are not meant to be read by minors anyway”, but the problem is far broader than that. In 1995 there was a flurry (eg <http://www.independent.co.uk/news/julia-somerville-defends-innocent-family-photos-1538516.html>) of stories about photograph developers reporting parents over image of their children. The switch to digital photography has merely meant that such images do not need developing. Many of them then find their way onto social media.

“HOW BEST TO PROTECT MINORS ...”

10. The Select Committee asks about “minors”. There is no known technology which will determine if a computer, or other device, is being used by a minor. For a home broadband connection, it would be possible for the purchaser to be asked whether there was likely to be a minor using the connection, but of course it is possible for the purchaser to lie, or even be honestly mistaken, as when suddenly looking after grandchildren.

11. Greater availability of, and publicity about, “parental controls” (which in fact are not parental at all, but the parent buying into some-one else's controls), on the lines of that offered by UK Safer Internet Centre,³⁴ would help. However, it is worth recalling two fundamental statements from their site: *“filters can be a helpful*

³⁴ <http://www.saferinternet.org.uk/advice-and-resources/parents-and-carers/parental-controls>

tool in **reducing** the chances of coming across something upsetting” and “remember that filtering is only part of the solution”.

12. A more challenging problem is provided by public WiFi technologies, which are used, often without accounts, or via accounts with no verification. Public convenience would seem to demand this light-touch access. It would be technically possible to have parental controls, although BCS does not necessarily recommend this would affect all users and could lead to a rapid spread of evasion technology.

13. Similar to parental controls on the connection, greater publicity about tools such as Google’s Safe Search³⁵ would help, but again it is worth noting a fundamental statement: “*please note that no filter can replace a watchful eye*”.

“... FROM ACCESSING ADULT CONTENT”

14. One problem which complicates the issue is that there is no international agreement about what constitutes “adult” content. Social norms vary widely and it is unlikely that there will be much consensus in the near future.

15. Content which has been formally rated “adult” in the UK is not a major problem. That content typically requires purchasing, for instance, via a credit card or PayPal account and the transaction will show up. A greater problem is pirated copies of such material, which are therefore not formally classified. The worldwide digital content industry is working hard to combat such piracy and this should be viewed as an international problem based on the fundamentally international character of the internet. BCS therefore does not see that UK centric action is likely to be helpful.

16. A particularly worrying development is the prevalence of truly home produced material by apparent minors. In one four-week period, the Internet Watch Foundation³⁶ (IWF) had 12,224 such images reported. 88% of these were on “parasite” (IWF terminology) websites, ie those that harvested such material from the website to which it was originally uploaded.

EDUCATION

17. The Byron report made a powerful analogy: “At a public swimming pool we have gates, put up signs, have lifeguards and shallow ends, but we also teach children how to swim”. To this one could well have added “and we help parents to teach children to swim, and we teach parents to be lifeguards.”

18. The sort of education necessary here for children is not technology education, it is societal education. For this reason BCS believes that it belongs in the general Personal, Learning and Thinking Skills (PLTS) category, rather than in ICT- or Computing-specific classes. There is excellent advice at the Get Safe Online website, and class templates such as <https://www.isc2cares.org/safe-and-secure/are> available.

19. The IWF’s comment on the home-produced material points again in this direction. “These findings provide evidence to support the importance of the education work delivered by child protection agencies to raise awareness of the permanence of information on the internet and the risks inherent to young people in creating and distributing this type of content.”

20. A challenging question is what and how much education is appropriate for parents. Some advice and help on “parental controls”, both on the configuration and on tools such as Google Safesearch³⁷ and YouTube’s SafetyMode,³⁸ most of which have come along since parents first encountered the Internet, is also appropriate. Similarly, parents need to become aware of the (excellent, and recommended in the Byron report) PEGI rating system for games and the advice at <http://www.askaboutgames.com/>, another site which has emerged since many parents learned about the internet and which recent learners will not necessarily come across. Schools should probably be encouraged to facilitate and host such classes in the PTA context.

21. Such classes will certainly need to cover technology, but should probably be wider. Parenting guidance is sometimes sought where parents would like support in terms of how to engage with their children on social topics that children might explore on the internet. These social topics are all related to what we might class as “growing up on the internet” and have security facets to them. Topics might include; management of friendships mediated by the Internet, trolling and other forms of Internet mediated abuse, balancing internet mediated activities with offline activities, identity and projection of self via the internet etc. Again, Get Safe Online has good age-specific materials, but these need to be drawn to the attention of parents, and their attention refreshed as the children grow older.

“FILTERING OUT EXTREMIST MATERIAL, INCLUDING IMAGES OF CHILD ABUSE AND MATERIAL INTENDED TO PROMOTE TERRORISM OR OTHER ACTS OF VIOLENCE”

22. This is already done to a significant extent in the area of child abuse (technically speaking, indecent images of children, which are illegal to possess under the Protection of Children Act 1978) by use of

³⁵ <https://support.google.com/websearch/answer/510?hl=en>

³⁶ <https://www.iwf.org.uk/>

³⁷ <https://support.google.com/websearch/answer/510?hl=en>

³⁸ <https://support.google.com/youtube/answer/174084?hl=en-GB>

blacklisting technology. More support could be given to the people, largely volunteers, who do the initial reporting, and to the blacklisting process, generally under the auspices of the IWF. It is worth commending the extent to which ISPs and mobile operators already cooperate with the IWF to manage and apply these blacklists.

23. It should be noted that blacklisting is not free, and has both financial and non-financial costs:

- (a) The ISPs need to install and operate substantially more powerful equipment to do filtering than is needed to pass through requests unexamined;
- (b) The ISPs, very largely, fund the IWF;
- (c) There is a risk of error and “false positives”: one such prevented edits to the whole of Wikipedia;
- (d) It is difficult to get right: the Irish study of filtering in schools;³⁹ showed that 50% of schools reported that filtering occasionally blocked valid educational sites, with a further 20% reporting that it regularly did so;
- (e) Filtering encourages the use of bypasses.

24. There has been much resistance to the Internet Watch Foundation’s widening its remit to the other material in the Select Committee’s question, and BCS does not believe that this is the way forward.

25. Some people say that more should be done, and imply, without saying so, that **content-based filtering** should be used, so that more such material could be blocked. This would require a major change in society’s attitude to censorship, as well as primary legislation to enact fundamental changes to the Regulation of Investigatory Powers Act. BCS does not believe that this is either feasible or desirable.

PREVENTING ABUSIVE OR THREATENING COMMENTS ON SOCIAL MEDIA

26. There has been much publicity recently around “online bullying”. Again, the problem is largely societal rather than technological. The recent publicity has forced some developers into adding “report abuse” buttons, but that is of little use unless the victims have the courage to do so. Hence this really comes down to an education question, see above.

27. Even in cases where there is not a “report abuse” button, it is important that social media service providers provide **clear** guidance and support for victims of distressing communications. These should detail methods for locating support and information on how to report the incident(s). Where possible and appropriate, providers should maintain regular contact with support and criminal justice agencies.

28. It is vital however, that the distinction is understood between those communications which:

- (a) Amount to threats of violence.
- (b) Targets an individual, resulting in harassment or stalking within the meaning of the Protection from Harassment Act 1997 (including two new criminal offences of stalking added as sections 2A and 4A to the Act by the Protection of Freedoms Act 2012).
- (c) Amount to a breach of a court order.
- (d) Those not covered by the provision above but may be considered grossly offensive, indecent, obscene or false.

29. In particular, given the evidence of the significant impact of the first three categories (including recent evidence on the impact of cyber stalking) we must ensure that such actions are not simply considered as grossly offensive and are dealt with under the appropriate legislation.

30. These categories are discussed in the *Guidelines on prosecuting cases involving communications sent via social media* from the Director of Public Prosecutions published on 20 June 2013.

31. Without the public having a clear understanding of the differences in these communications the problem is unlikely to diminish. Digital Natives have embraced technology but unfortunately without appropriate training and education they struggle to understand the social norms of internet communication and behaviour.

32. There is a clear issue around anonymity and perceived anonymity (as well as untraceability) in social media.

- (a) In cases where senders of malicious communications have anonymity and (practical) untraceability there can be difficulty in bringing justice and technological and legal changes may be needed.
- (b) In cases where senders have a (mistaken) perception of anonymity or untraceability they may display fewer inhibitions and feel beyond reproach. It is important that all those who can assist in making communications more traceable, particularly by giving up log information, do so fully and readily when requested by those in the criminal justice system. The recent changes to the Protection from Harassment Act 1997 do give police further powers and this is a welcome change.

³⁹ <http://tnc2007.terena.org/programme/presentations/show4fa0.html>

- (c) Where receivers of abusive messages perceive (rightly or wrongly) anonymity or untraceability of the senders they may feel there is little point in reporting the communication, even when it has significant impact.

33. It is important all stakeholders consider the vulnerability of the victim in cases of abusive or threatening messages.

CONCLUSION

34. As a charity whose mission is “*to enable the information society*”, BCS looks forward to being a significant player in society’s development of answers to these questions and welcomes continued dialogue.

September 2013

Written evidence submitted by Dudley Friend Clayson

I write as an independent & individual contributor of evidence to this Inquiry.

I am the retired Chief Executive of a company supplying UK industry with packaging machinery & consumables. My wife is a retired doctor. Our evidence will cover the following issues:

- How our family has taken the initiative in safeguarding against the danger of our children accessing pornographic material online.
- How members of our church have coped with this danger and cared for those who have been mentally and morally damaged by it.
- Measures that Government should put in place to ensure that minors are seriously protected from accessing pornographic material.
- Regulatory initiatives which OFCOM should take to regulate & police social media which are currently responsible for a significant volume of material totally inappropriate for exposure to minors.
- The internet industry must unite to develop technology to prevent the covert proliferation of such material amongst minors.

1. How did we cope? My wife & I raised our family of four children without a computer in our home. As practising Christians we could not, with a good conscience, expose our children to the possibility of coming in contact with the poison of adult pornographic material, which is morally destructive in its consequences and “utterly without redeeming social value” (1966 Supreme Court ruling in the obscenity case re. *Fanny Hill*, defining pornographic material).

2. Our children are now married, and have their own families. Both they and we all now have computers in our homes which are effectively filtered to eliminate any possibility of inadvertent contact with adult material by anyone in the household.

3. Implicit in this Inquiry is the Government’s acknowledgement that the exposure of minors to adult material is harmful. Such exposure entails grave consequences for the child, the family and for society at large. We are now seeing the social norms & stabilising values which have underpinned our customary way of life in this country being threatened by the emergence of a juvenile generation whose attitudes in respect of sexual gratification, sexual crime, violence, promiscuity and marriage are being distorted & perverted by exposure to online pornography. Sadly we have had some first-hand experience of damage to just a very few of the young people in our church who have temporarily had contact with this depraved material. It has required ongoing pastoral care & counselling to help them to get through the moral distress and mental disturbance resulting from this exposure. Pornography leaves a scarring in the mind. We trust that the effects will be short-term; but for some it could be a lifelong trauma.

4. It is heartening to see that Government is working with internet providers to put in place measures which will effectively protect minors from easy & instant access to adult material. The Prime Minister himself has given an undertaking that pornography will be automatically blocked on new broadband internet accounts, leaving viewers with the option to remove the filter if they so decide. Mr Cameron has also made a commitment in respect of existing users: the principal internet providers will have an obligation to contact customers with an “unavoidable decision about whether or not to install family friendly content filters”. He has indicated this will happen by end-2014. OFCOM will be responsible for implementation of these measures. The Prime Minister has promised to take further action if, following these steps, there is evidence that children are still not being effectively protected. We welcome his robust stance on this issue, which will mean that the many parents who would like to be prompted or reminded will get that reminder and will be shown very clearly how to put on family friendly filters. This is a positive move and a valuable commitment at the highest level in Government.

5. OFCOM should prioritise regulation of social media, such as Facebook, and chatrooms, where the content is not infrequently pornographic. OFCOM must ensure that the regulation & monitoring of these sites are significantly upgraded, with mandatory training & compliance regimes put in place. Social media should be

placed under specific obligation to delete offensive material swiftly whenever a viewer complaint is received. This is in essence a Health & Safety legislation issue and every other industry in which I have been active has been subject to the strictest compliance with HSE. The internet should be no exception.

6. OFCOM should recognise that social media are exploited by paedophiles, prostitutes and sex traffickers and should create an appropriately strong regulatory framework to block these criminal and anti-social abuses of the internet. OFCOM should also require social networking sites to implement effective & inescapable age verification checks to prevent minors accessing inappropriate material.

7. The internet industry should devote resources to develop technology to prevent the covert and currently uncontrollable circulation of adult material within minors' peer groups (such as school friend communities).

In conclusion, we are grateful for this Inquiry. The current situation is dire, with a reported 81% of 14–16 year olds having already accessed pornographic material online. We believe that < 50% of UK families currently have family friendly content filters in their home computers. The Government's commitments in response to this situation are encouraging. We and a wide circle of our friends in this country will be scrutinising progress and developments closely. We are very deeply concerned that the situation is rapidly brought under effective, ongoing control—for the sake of every young person and child in this country.

September 2013

Written evidence submitted by PAPYRUS Prevention of Young Suicide

SUMMARY

PAPYRUS has campaigned since 2004 for better regulation of the online promotion of suicide.

Amongst the many dangers posed by the internet, its use to promote suicide receives relatively little attention.

Young people, for whom the internet is a primary source of information, are particularly vulnerable to websites and chatrooms promoting suicide. For those young people who are suicidal or are vulnerable because of a mental health concern, such platforms can pose a particular danger.

The Government has made clear that the law which prevents encouraging or assisting suicide applies online as much as offline, but no prosecution for online assistance has been made in this country.

ISPs should block websites and chatrooms which deliberately promote suicide. In the absence of this parents should have to “opt in” to suicide sites in the same way as is proposed for other sites posing a danger to children and young people.

Bodies such as IWF and CEOP should include suicide within their remit—at present both exclude it.

DETAIL

1. PAPYRUS Prevention of Young Suicide is a national charity dedicated to the prevention of young suicide. Originally started by parents who had all lost a son or daughter to suicide it is now open to all who share our aims, although many of its members have personal experience of a young person's suicide.

2. Suicide is one of the biggest causes of death amongst young people; every year in the UK between 600 and 800 young people between the ages of 15 and 24 take their own lives—a number equivalent to the population of a small secondary school; under the age of 35, the number rises further. According to the ONS statistics published on suicides in 2011,⁴⁰ the total number of those who took their own lives before they reached 35 years of age was over 1700.

3. In the early years of the century, PAPYRUS became aware of several young people who had killed themselves after downloading information from websites giving specific information and advice on how to take one's own life and/or having participated in chatrooms where advice and encouragement was given on killing oneself. Since 2004 it has campaigned for the removal, or at least some regulation, of such sites.

4. Much of the public concern about the dangers of the internet has centred on its use to promote pornography, bullying, eating disorders and self harm; these are important areas of concern both in their own right and because they may play a significant part in leading vulnerable people to consider and attempt suicide. But the suicide sites themselves are uniquely dangerous in that they can—and do—lead directly to deaths of vulnerable young people. They also provide information which is not available from other sources. You will not find a book in W H Smith's describing in graphic and lurid detail the various ways of killing yourself; you *can* find this (sometimes with pictures) on the internet. And of course this can be accessed by children and vulnerable young people 24 hours a day, in the privacy of their own home or elsewhere from computers and other e-devices. My own son took his own life aged 17, after downloading such information from the internet.

5. For many young people the internet has become the primary source of information; coupled with the pressures of growing up, sometimes exacerbated by mental ill-health, there is a particular confluence of danger. And although PAPYRUS's particular concern is for young people many others who are vulnerable, again

⁴⁰ <http://www.ons.gov.uk/ons/rel/subnational-health4/suicides-in-the-united-kingdom/2011/stb-suicide-bulletin.html>

through mental illness or for other reasons, are also all too easily exposed to the dangers of the sites. When PAPYRUS began campaigning it knew of four young people who had killed themselves with the aid of the internet. Some time ago the number of internet-related suicides of which we were aware passed 50 and we are sure that this is a considerable underestimate—no figures are collected centrally and this figure was obtained merely through unofficial press monitoring. Many coroners have expressed concern about the impact of the internet in cases of suicide.

6. The 1961 Suicide Act made it illegal to aid, abet, counsel or procure a suicide. The Coroners and Justice Act 2009 amended the law by updating the language to refer simply to assisting and encouraging suicide, whilst making it clear that the law applies to online actions in exactly the same way as it does offline.⁴¹ PAPYRUS contends that sites and chatrooms promoting suicide may be illegal in that they can—and do—assist and encourage others to take their own lives; however no prosecution has taken place in this country.⁴² We believe that the Internet Service Providers (ISPs) should take action to block such sites in the same way as they do for other illegal sites, such as child pornography.

7. In his speech on 22nd July the Prime Minister called on the ISPs to provide to all new customers family friendly filters covering all devices in a household, which can only be switched off by the householder; and to extend this in due course to all existing customers—in effect an “opt-in” approach despite the fact that this has previously been eschewed by the Government. PAPYRUS warmly welcomes the Prime Minister’s intervention and believes that the filters must automatically block dangerous sites and chatrooms which promote suicide. (TalkTalk has told us that the category most blocked by parents using their existing filters is suicide/self harm.) We have written to the Prime Minister seeking his assurance that the suicide sites will be encompassed within these new arrangements. We trust that this will have the support of your committee also.

8. The internet can, of course, also be beneficial in countering suicide and in providing support to those who are suicidal; PAPYRUS’s own helpline⁴³ provides professional advice and information by telephone, email or text messaging, to those concerned that a young person may be at risk of suicide and to young people who are themselves having thoughts of suicide. It has sometimes been argued that any blocking of harmful suicide sites must of necessity also block helpful sites; we have always believed that it is perfectly possible to retain access to the helpful sites and were pleased to note that the Prime Minister acknowledged this in his speech and has asked UKCCISS to lead work to ensure that this is so. We stand ready to assist in this work.

9. Although these recent advances have focussed on protecting children and the young (and we warmly welcome them as such) we believe that the dubious legality of the websites and chatrooms provides sufficient grounds for ISPs to block them for all users. There is also a moral justification for doing so; anyone seeking access to them is likely to be vulnerable, either generically or at that particular time.

10. One of the proven ways of reducing suicides is to limit access to the means of killing oneself. This is highlighted in the current National Suicide Prevention Strategy in Area for Action 3⁴⁴ and a recent study has confirmed the effectiveness of limiting the numbers of paracetamol sold in individual packets.⁴⁵ The National Suicide Prevention Strategy for England states (para3.3) that “The internet is a ready source of detailed information concerning the use of lethal suicide methods.” The young and vulnerable can and should be protected from easy access both to information on the means of killing themselves and indeed to the means themselves, through suicide paraphernalia and kits sold online.

11. One of the difficulties in pursuing the dangers of suicide promotion online is that there is no central body to which relevant concerns can be expressed. Neither the industry body—the Internet Watch Foundation (IWF)—nor the Government’s Child Exploitation and Online Protection Centre (CEOP) regards suicide as falling within their remit. We have asked repeatedly for this to change and believe that real benefits would ensue if this were to happen.

September 2013

Written evidence submitted by EU Kids Online

PREAMBLE

We note with interest that the Culture, Media and Sport Committee has decided to investigate a number of aspects of online safety that are currently raising concerns, in particular:

- How best to protect minors from accessing adult content.
- Filtering out extremist material, including images of child abuse and material intended to promote terrorism or other acts of violence.
- Preventing abusive or threatening comments on social media.

⁴¹ Ministry of Justice Circular 2010–03

⁴² A former nurse has been convicted in Minnesota of assisting suicide online, including that of one person in England

⁴³ HOPELineUK 0800 068 41 41

⁴⁴ https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/216928/Preventing-Suicide-in-England-A-cross-government-outcomes-strategy-to-save-lives.pdf

⁴⁵ <http://www.bmj.com/content/346/bmj.f403>

This response is written by Professor Sonia Livingstone, on behalf of the EU Kids Online network.⁴⁶ This response may be made public. The address, for a copy of the Committee's report, is S105, Department of Media and Communications, London School of Economics and Political Science, Houghton Street, London WC2A 2AE.

Much of EU Kids Online's work has focused on scoping the nature and consequences of the online risks of harm encountered by children aged 9–16 years old in Europe. The detailed recommendations below relate to the European findings detailed on our website.⁴⁷ For UK-specific findings, see Livingstone, S *et al* (2010). *Risks and safety for children on the internet: The UK report*. At <http://eprints.lse.ac.uk/33730/>

SUMMARY

The strength of a cross-national study is that it reveals how the UK measures against other European countries. In many respects, the UK has been a leader in protecting children against online risk of harm. However, EU Kids Online's cross-national analysis also reveals that this protection has often come at the cost of empowering children to benefit from the digital skills and opportunities of new online technologies. Specifically, we found that European countries divide into four main groups, based on children's risk profiles: Supported risky explorers; Semi-supported risky gamers; Protected by restrictions and Unprotected networkers.

In Belgium, France, Germany, Greece, Ireland, Italy, Portugal, Spain, Turkey, **and the UK**—the “protected by restrictions” countries, parents tend to overprotect their children, significantly reducing their online opportunities. Researchers are concerned that both too much parental restriction and the lack of support for children's online use might lead to higher levels of harm when risk is encountered. Hence the EU Kids Online network consistently emphasises that policy to encourage opportunities should accompany policy to reduce risk of harm.

MAIN POINTS

1. Children have the right to protection and safety online but they must also take responsibility for keeping safe and respecting the rights of others online

1.1 New means of internet access, less open to adult supervision, are increasingly evident in young people's internet use. Nearly half of all children in Europe go online in their own bedroom where it is unrealistic to expect parents to monitor their safety.

1.2 Children need to be encouraged to develop self-governing behaviour in which they take greater responsibility for their own safety in the use of the internet.

1.3 Awareness-raising should emphasise empowerment rather than restriction, and appropriate, responsible behaviour with regard to technology use.

2. A new focus is needed on internet safety for younger users

2.1 It is important to balance protection of younger users with opportunities. It is important not just to make the online world safe by stopping their use of internet services, but also to ensure their participation in safe ways.

3. Safety messages should be adapted to new modes of access

3.1 33% of children now go online via a mobile phone or handheld device. Laptops, mobile phones, game consoles and other mobile devices allow children to go online anywhere, anytime, away from parental supervision. Emerging services (such as location-based ones) may lead to new risks.

4. Children's online opportunities and skills need human and financial investment

4.1 Not only do younger children and girls not progress as far up the “ladder of opportunities” as teenagers and boys, many never reach the final set of activities at all. Only half of 9–10 year olds progress further than basic content-related activities.

4.2 Promoting more creative and skilled applications is essential to ensure all children avail of online opportunities.

4.3 Schools play a pivotal role in digital skills development, mitigating forms of digital exclusion. However, teachers are often inadequately resourced and trained to carry out the functions entrusted. Country differences in online skills point to the need for targeted educational interventions where there is evidence of a digital divide.

4.4 Since opportunities and risks online go hand in hand, efforts to increase opportunities may also increase risks, while efforts to reduce risks may restrict children's opportunities. A careful balancing act, which recognises children's online experiences “in the round”, is vital.

⁴⁶ <http://www.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx>

⁴⁷ <http://www.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx>

5. Positive online content for children should be made a policy priority

5.1 Provision of appropriate—high quality, diverse content online should be a priority.

5.2 The “European Award for Best Children’s Online Content” is a valuable step in this direction, but such provision could also be supported by high profile national initiatives.

6. Digital safety skills are needed to build resilience online

6.1 Inequalities in digital skills persist—in terms of SES, age and, to a lesser degree, gender, so efforts to overcome these are needed.

6.2 Younger age groups need to be a particular priority for parents and teachers. Secondary level schools to date have been the main providers of ICT skills training but new interventions are required at the primary level.

6.3 Encouraging children to do more online will also improve their digital skills as well as their overall confidence and/or increasing children’s beliefs in their abilities to use the internet. Similarly, teaching safety skills is likely to improve other skills, while teaching instrumental and informational skills will also improve safety skills.

6.4 Given uneven digital skills, particularly safety skills, across Europe and the discussion among stakeholders about the need to identify more precisely the kinds of skills required, an inventory and agreed framework for digital safety training would provide a valuable resource for educators, awareness-raising and civil society groups.

6.5 Schools are uniquely placed to reach the maximum number of children. They are regarded by parents as the most trusted source of information and, as the second most common location for going online, they provide children with a very important point of access.

7. Social networking service providers need to ensure that maximum protection is provided for the accounts of minors

7.1 If SNS age restrictions cannot be made effective, the de facto use of SNS by young children should be addressed so as to ensure age-appropriate protection.

7.2 Privacy/safety settings and reporting mechanisms should be far more user-friendly. If they remain difficult to use, privacy/safety settings should be enabled by default.

7.3 Digital skills to protect privacy and personal data should be strongly supported among children of all ages.

7.4 It should also be noted that one in three parents (51% of parents of 9–12 year olds, 15% of parents of 13–16 year olds) did not wish their child to use SNS.

7.5 The review of data protection legislation at a European level needs to be considered from the point of view of children’s privacy.

8. Awareness-raising in relation to online risks should be balanced and proportionate, and targeted at those most at risk of harm

8.1 Children are concerned about a wide range of online risks. Efforts to manage these risks, and to support children in coping with them, should maintain a broad and updated view of these risks.

8.2 As 9% of 9–10 year olds have been bothered or upset by something on the internet in the past year, it is important to promote awareness-raising and other safety practices for ever younger children.

8.3 Awareness-raising among teenagers and their parents and teachers remains a priority since upsetting experiences rise with age and the array of risks keeps changing.

9. Parental awareness of risks and safety online needs to be enhanced

9.1 Without being alarmist or sensationalist, parents need to be alerted to the nature of the risks their children may encounter online. Awareness-raising should try to encourage dialogue and greater understanding between parents and children about young people’s online activities.

9.2 Increasing parental understanding of risks is particularly important in those countries where awareness of children’s risk experience is lowest.

10. Responses to young people’s exposure to online sexual content needs to be proportionate and should focus on those most likely to be distressed or harmed by such exposure

10.1 Although public concern over online sexual content is justified, the extent of children’s exposure should not be exaggerated, and nor should it be assumed that all children are upset or harmed by such exposure.

10.2 Although the internet makes sexual content more readily available to all, with many children reporting exposure via accidental pop-ups, the regulation of more established media (television, video, magazines, etc) remains important.

10.3 Private access also matters—children who go online via their own laptop, mobile phone or, especially, a handheld device are more likely to have seen sexual images and/or received sexual messages. Similarly, those who go online in their bedroom, at a friend's house or "out and about" are more likely to see sexual content online. The early advice that parents should oversee children's internet use must be revised, and new safety tools are needed.

10.4 It seems that popular discourses centred on teenage boys' deliberate exposure to sexual content makes it harder for parents and others to recognise the distress that inadvertent exposure may cause girls, younger children and those facing psychological difficulties in their lives.

11. Sensitive responses to bullying are required with equal attention to online and offline occurrence

11.1 In countries where there is more bullying overall, there tends to be more bullying online. This suggests that as internet use increases, so will bullying online. Thus anti-bullying initiatives should accompany efforts to promote internet use.

11.2 Online and offline bullying should be seen as connected, part of a vicious cycle in which perpetrators reach their victims in diverse ways and victims find it hard to escape.

11.3 Those who bully may also be vulnerable, and they are often victims themselves, so sensitive treatment is required.

11.4 Although children have a range of coping responses, cyberbullying upsets them, and more support and awareness-raising is needed. Fewer than half tell a parent or other adult, and fewer than half know how to block the person or delete their messages.

12. Parents need to be more aware of the practice of offline meetings with contacts first made online

12.1 It is important to distinguish making new contacts online—a common occurrence—from going to meet new online contacts offline. It is equally important to recognise that for the most part, meeting online contacts offline is harmless, probably even fun.

12.2 But for a minority of children, meeting online contacts offline is harmful, and these children tend already to be the more vulnerable.

12.3 Since their parents are often unaware of what has happened, awareness-raising efforts should be increased so that parents of younger and/or more vulnerable children recognise the risk, but without this undermining the chance for most children to have fun making new friends online.

13. Policy makers need to be alert to new risks that affect children and young people, especially arising from peer-to-peer contact

13.1 As well as conducting surveys, qualitative work based on listening to children is vital to learn what new risks they are experiencing.

13.2 Addressing risks associated with peer-to-peer conduct (user-generated content and personal data misuse) poses a critical challenge to policy makers.

13.3 While younger children have fewer resources to cope with online risk, they are also more willing to turn to parents for help. Meanwhile, teenagers face particular risks that worry them and that they may struggle with alone, so they need particular coping strategies and support.

14. Awareness-raising should highlight effective coping strategies in safety messages, emphasizing social supports such as talking to parents, friends and teachers, as well as the use of online tools

14.1 Policy makers have long advised children to tell someone if they've been upset online, and it seems such messages have been heard.

14.2 Children try some proactive strategies more than others and few are fatalistic. This suggests a desire to cope as best they can and a readiness to adopt new technical tools if these are accessible.

14.3 When asked which strategies really helped the problem, children say that reporting the problem to an ISP was effective with sexual images but less so for sexual or bullying messages: this suggests that better solutions are needed for peer-to-peer risks.

14.4 Mostly, children said the approach they chose helped in up to two thirds of cases, but this leaves room for provision of better support and/or tools.

14.5 It seems that efforts to promote children's digital citizenship—in terms of online safety and good practice—are bearing some fruit, and should be extended. There may be many reasons why solutions children

try, when upset, do not help the situation, but one possibility is that the technical tools are flawed or difficult to use, and another is that adults—professional or personal—are unprepared or unable to help children.

14.6 The “knowledge gap” phenomenon—in which the information-rich learn from available advice and guidance more rapidly than the information-poor—means that efforts to promote digital citizenship will disproportionately benefit the already-advantaged. Targeting less privileged or more vulnerable children is a priority.

14.7 Overwhelmingly, children tell a friend, followed by a parent, when something online upsets them. Rarely do they tell a teacher or any other adult in a position of responsibility. Their apparent lack of trust in those who may have more expert solutions is a concern.

15. Practical mediation skills for parents should be a part of the overall effort to build awareness among parents of risks and safety online

15.1 Parents appear to have got the message that it is valuable for them to engage with their child’s internet use, and they employ a wide range of strategies, depending partly on the age of the child. But there are some parents who do not do very much, even for young children, and there are some children who wish their parents to take more interest. Targeting these parents with awareness-raising messages and resources is thus a priority.

15.2 Cynicism that what parents do is not valued, or that children will evade parental guidance, is ungrounded: the evidence reveals a more positive picture in which children welcome parental interest and mediating activities while parents express confidence in their children’s abilities. It is important to maintain this situation as the internet becomes more complex and more embedded in everyday life.

15.3 Parental restrictions carry a significant cost in terms of children’s online opportunities and skills, but they may be appropriate if children are vulnerable to harm. Parental efforts to empower children online seem to enhance their opportunities and skills, though there is little evidence that they reduce risk or harm. Since there are no easy answers, parents should be supported in judging what best suits their child.

16. Filtering technologies and parental control software need to be far more usable and transparent and take into account the needs of parents in order to improve uptake

16.1 Across the 25 countries surveyed by EU Kids Online, less than one third (28%) of parents were found to filter the websites visited by their child. It is clear that many parents find such software either too complicated or ill-suited to their needs.

To be effective, parental controls need to incorporate all of the issues that concern parents about their children’s internet use. Thus, in addition to filtering out adult or unsuitable online content for children, controls may also need to include features such as the amount of time spent online, filtering of user-generated content and blocking of commercial content.

While there continues to be debate about the appropriateness of parental controls in all situations, they continue to be a valuable resource particularly for those who may lack skills or knowledge in advising on and guiding their children’s internet use.

Parental controls are also available as an integral element of some internet services and do not need to be separately installed. An industry-wide agreement on the design and features of safety and parental controls built into web-based services could provide parents with better opportunities to consider adopting them. Training in the use of tools should also be made readily available to deal with lack of confidence and knowledge on the part of parents.

17. Levels of teacher mediation are high but could be higher, as a large minority of children are not reached by teacher guidance. Since schools have the resources to reach all children, they should take the biggest share of the task of reaching the “hard to reach”

17.1 The youngest children (9–10 years) report the least mediation from teachers: as this age group now uses the internet widely, primary schools should increase critical and safety guidance for pupils.

17.2 The benefits of supporting peer mediation are easily neglected but could be constructively harnessed, especially as children are most likely to tell a friend if something bothers them online. Peer mentoring schemes have a valuable role to play.

17.3 When something has bothered them on the internet, 36% of children said a parent helped them, 28% a friend and 24% a teacher. The ideal may for children to have a range of people to turn to, depending on the circumstances. A minority of children has no-one to tell when something upsets them.

18. Industry needs to be much more proactive in promoting internet safety awareness and education. In order to increase trust, the management of safety, identity and privacy settings of internet services used by children needs to be transparent and independently evaluated

18.1 The overwhelming majority of parents would like to receive information and advice about internet safety. Most, however, get it from firstly from family and friends (48%) rather than from the providers of internet services. Traditional media (32%) and the child's school (27%) are the next most common sources of information about internet safety. Internet service providers (22%) and websites (21%) are much less evident as sources of advice.

18.2 There is considerable scope, therefore, for industry to improve its own awareness raising and provision of safety advice. Internet safety advice should be provided in an accessible and user-friendly way at the point of access on web services used by young people. Internet service providers (ISPs) should play a more prominent role in providing online safety resources for parents as the primary account holders.

18.3 Traditional media sources—press, radio and television—also have a major role to play in promoting online safety awareness as supporting greater media literacy among the adult population. They are best positioned to reach all adults and, crucially, are influential in forming parents' attitudes towards opportunities and risks on the internet.

18.4 Evidence repeatedly shows that children still struggle with user tools, safety devices, privacy settings and policies, reporting mechanisms, etc, even though the industry claims they have been improved and made easier. Independent evaluation of progress by the industry is crucial, to measure whether improvements have been made (against benchmarks) but more importantly, whether those improvements work—ie are they actually sufficient for children to manage their safety, privacy, identity and risk online?

September 2013

Written evidence submitted by Rolf Smith

BACKGROUND TO SUBMISSION

Firstly, I would like to thank the Government for giving me the opportunity to provide this submission to the Committee.

I am 33 years old and am happily married to my wife; of whom we have two children aged seven and five. I am writing therefore in my capacity as a father with some experience, as well as with feelings for all fathers and mothers of children throughout the UK and across the globe. As a parent I am acutely aware of the many potential threats to our children's safety, of which the internet is an ever present and increasing one; hence the reason for this submission.

Whilst I am not a professional or seasoned campaigner, I can honestly say that the following information is given in good faith and is believed to be correct. Any data provided was taken from Ofcom reports.

PERSONAL EXPERIENCES AS FATHER OF A YOUNG FAMILY

Computers and the internet are a fundamental part of life for our children, as they are for any children in the UK today. In a way that we adults did not, they are growing up with computer technology all around them. Indeed, it is astounding how quickly—almost naturally—they pick it up. My daughter has just turned five and cannot yet read, but even she can navigate with remarkable speed through websites she knows to find the part she wants, simply by memorizing the position of the links and buttons! It is abundantly clear and proven that the internet appeals to a child's inquisitive nature and their exploratory learning style; certainly that has been our experience, and it won't be long before they are better at it than us.

There is no doubt that the internet can be useful for children, particularly we have found it helpful for improving parts of our older child's education. But we are *very* thankful for the strong filters we have in place which allows access to approved sites only. This gives my wife and I the opportunity to check the content of sites carefully before allowing them to be visited by our children. Even so, our children are only allowed to access the internet for timed, monitored periods and we certainly wouldn't leave them alone during this time. I know and they know—as we have taught them—that the internet has hidden dangers that they are not able to cope with.

In addition, too much computer activity tends to make our children less interested in outdoor activities and other necessary skills like writing and drawing.

THE NATIONAL SITUATION REGARDING ONLINE SAFETY

The Committee will no doubt be aware of the many statistics published by Ofcom on the subject of children and safety online. Therefore it is not necessary for me to go into too much detail regarding the national situation; however I must point out that it is very clear from data gathered that many parents in the UK, unlike myself and my wife, are relatively unaware of how potent the hidden dangers of the internet are. While most parents acknowledge that there should be some form of parental control, many do not view the potential

dangers as particularly serious so are not pro-active in controlling their children's use; therefore they allow their children to spend long periods online alone without supervision and without controlling software. This key fact could have a serious negative impact on UK society in the future if it is not properly addressed now. This is of great concern to me. A few key Ofcom findings bear this out:

- 54% of parents in the UK do not use parental control software on their home internet.
- 46% of parents agree that their children know more about the internet than they do.
- 81% of children aged 14–16 have viewed adult material online.
- Only 17% of parents say they are concerned about the internet.
- 25% of 8–11 year olds and 34% of 12–15 year olds are likely to communicate with people not directly known to them via social networking sites, these figures rose greatly in 2012 report.

WHY ONLINE SAFETY FOR CHILDREN IS AN ISSUE WHICH NEEDS ACTION

It is undoubtedly a necessity that children are kept safe from harm wherever they are, and this must include when they are on the internet. The proliferation of social networking, video sharing, personal smartphones etc has made it even more vital that this issue is viewed seriously. The reality is that practically every UK child is using the internet, and 80% of 12–15 year olds in the UK have an online profile. Therefore children must be actively protected from the following (among others):

- Access to explicit adult material.
- Online grooming and other harmful communications.
- Cyber bullying.
- Online stranger danger.
- Uncontrolled spending.

It seems from Ofcom data that the issue is twofold:

- (a) While most parents know that the internet has dangers, many do not consider them to be serious enough to pose a significant risk to their children. Therefore there is a *lack of awareness*.
- (b) This has meant that *parental control software*, which is essential to maintain safety for children on all online devices, is not used nearly as widely as it needs to be.

SUGGESTIONS OF ACTIONS THAT COULD BE TAKEN TO IMPROVE ONLINE SAFETY

As is the case for the care of children generally, the ultimate responsibility for ensuring children stay safe online lies with their parents. Parents need to speak to their children about online safety, impose restrictions and controls, and maintain supervision at all times. However, there are two things that I feel Government must do fulfil their part in addressing the issue of Online Safety for children:

- (1) *Increase parental awareness*—the dangers of the internet do often seem remote and hypothetical, whereas they are in fact very real and present. Government can use its considerable influence to help parents across the UK to realize this. Parents need to be helped to understand that it is a basic responsibility to protect their children online, as much as it is basic to teach them how to cross the road safely.
- (2) *Insist on parental control software*—rather than leaving parents to investigate and install some kind of control software, Government must insist that every online device sold in the UK for personal use must come with parental control software pre-installed. Ofcom's findings absolutely support this suggestion. They found that the primary reasons given for parental controls not being used were as follows:
 - (a) a lack of awareness or gaps in understanding;
 - (b) the perceived complexity of parental controls;
 - (c) the degree of effort that was expected to be required; and
 - (d) busy lives coupled with the absence of a specific trigger.

In addition to this, Ofcom reports that “when parents were asked whether they would install parental controls if the process was made very easy, almost all parents said they would do so.”

I look forward to hearing the results of the Committee's inquiry, and look forward to hearing about the Government action which is sure to follow.

Many thanks again for the opportunity to provide this submission.

September 2013

Written evidence submitted by Mediawatch-UK

A. EXECUTIVE SUMMARY

1. We welcome recent government initiatives designed to protect minors from accessing adult content but are of the opinion that three key areas must still be addressed in order to provide the best possible protection. These are:

- Education.
- Age verification.
- Statutory backing.

2. We welcome discussion of how best to prevent abusive and threatening behaviour using social media. This is a behavioural issue and unlikely to be effectively dealt with by filtering but by collaboration between industry and other stakeholders. We believe there are three key areas in tackling this problem:

- Education.
- Regulation.
- Real sanctions, with statutory backing if necessary.

B. MEDIAWATCH-UK

3. Mediawatch-UK is a voluntary organisation, established in 1965 by Mary Whitehouse CBE and formerly known as the National Viewers' and Listeners' Association. Mediawatch-UK has thousands of subscribing members throughout the UK. Our membership consists of people of all ages, occupations and backgrounds who are concerned about the overall influence of the media on the individual, the family and wider society.

4. Our Director and other spokespersons appear regularly in the media (press and broadcast) on behalf of our members. Further information about Mediawatch-UK can be found on our website: <http://www.mediawatchuk.org.uk/>

C. HOW BEST TO PROTECT MINORS FROM ACCESSING ADULT CONTENT

5. We believe that parents and businesses have a shared responsibility for children's online safety. Parents/guardians have the ultimate responsibility for their children but businesses and government have a responsibility to provide parents with the tools they need to keep their children safe.

Education

6. Many of our members have reported difficulty with installing content filters and keeping up to date with filters across the plethora of internet-enabled devices in their homes. Coupled with this many have reported confusion in knowing where to go to access reliable information and education on internet safety.

7. This is best illustrated by a family which recently contacted us for help. The family fostered children whose chaotic backgrounds placed them at particular risk. They were long time carers for a child who had suffered a history of serious sexual abuse. They were aware of the potential risks online and had taken advice from social services and their ISP. They had set up filters on the internet enabled devices in their home and believed their mobile devices would be protected under The Mobile Broadband Group Code of Practice. Their child was introduced to pornography on the phone of a child at school and she soon became addicted and was regularly accessing pornography using the wi-fi at the homes of friends using her phone. Because of this child's history she is particularly vulnerable to sexual exploitation and misadventure.

8. At the time of the Parliamentary Enquiry into Online Child Protection in 2011 we asked our members (a group likely to be more than averagely engaged with this issue) whether their ISP had ever contacted them with details of the parental controls available as part of their package.

- 20% reported that their ISPs had informed them about parental controls.
- 80% said their ISPs had never done this.
- Of those who had been told about parental controls 61% were with TalkTalk. Approximately 60% of TalkTalk subscribers had been alerted to their provider's new HomeSafe service.
- Of members who subscribed to other services only 11% had been told about the parental controls available.

Of some concern were a number of BT customers who were under the impression that installing parental controls would cost them a further subscription.

9. There is a great need for integrated and accurate advice for parents and carers on the potential dangers of accessing inappropriate online content and how best to protect their children. There is much good work being done in this area by a variety of organisations but further co-ordinated work is required to ensure that all parents are made aware of and receive access to information and assistance.

10. We believe there should be space in sex and relationship education in schools to educate young people about the potential dangers of accessing adult content online, how to avoid doing so and strategies to enable them to understand what they may have seen.

Age verification

11. We welcome the Government's efforts in this area but believe no mechanism ("active choice", "default-on" or "opt-in"), will work without "robust age verification".

12. We commend efforts made in the internet gambling industry to all but eradicate underage online gambling and we would like to see similar measures implemented with regard to adult material with appointed agencies, possibly OFCOM or ATVOD, regulating.

Statutory backing

13. We also remain convinced that the best approach to ensure the Government's pledges are actually delivered on is by changing the law. The current "default-on" proposal is a voluntary agreement between the major ISPs and, although four currently dominate the market, the Government's plan does leave around 10% of the market unaccounted for. If filters were legislated for then all ISPs and MPOs, regardless of size, would have to conform which would offer a greater degree of protection.

14. Statutory backing would also remove anomalies between different providers and contracts. For example: many consumers believe that, as a result of the Mobile Broadband Network's code, child filters are activated as a default for all UK mobile phone customers. This is not the case. Some providers require the filters to be activated and provision varies dependent on whether a phone is pay-as-you-go or contract, provided by a Mobile Phone Operator or a Mobile Phone Virtual Operator.

D. PREVENTING ABUSIVE OR THREATENING COMMENTS ON SOCIAL MEDIA

Education

15. There is a great need for integrated and accurate advice for users, parents and carers on the potential pitfalls of social media use and how best to protect themselves and their children. There is much good work being done in this area by a variety of organisations but further co-ordinated work is required to ensure that all parents are made aware of and receive access to information.

16. We believe there should be space in PSHE education in schools to educate young people about safe and responsible social media use including the consequences of anti-social behaviour and sources of advice and support in case of abuse.

Regulation

17. The former Director of Mediawatch-UK, John Beyer, during the course of his work attracted much criticism including an abusive Facebook page entitled "I Hate John Beyer". When this was brought to our attention we reported it Facebook and asked for it to be removed. We reported the page three times but heard nothing back from Facebook. Eventually, after approximately three months, the page was removed although we were not formally informed of its removal but discovered it ourselves.

18. Although the issue was dealt with it took too long and there was not enough communication in the process. Neither were we directed to sources of support and advice. These are issues which need to be addressed in a code of practice for social media sites.

19. Social media is now a mature medium and it is our opinion that it should be regulated accordingly. Recent events (such as the suicide of Hannah Smith following bullying on ask.fm) have demonstrated the potential effect of online abuse. We believe that abusive and threatening behaviour on social media is now an issue of health and safety and we would like to see it regulated accordingly via an industry code of practise.

20. We would like an independent regulator to ensure that sites are sufficiently moderated and that complaints are dealt with swiftly, efficiently and within an agreed timeframe. Such a regulator could ensure the development and implementation of an industry code of practice with the results promoted to parents and children. This code should include:

- Clearer and simpler reporting mechanisms, especially where a service is marketed at and provided to under 18s, making it easier for users to report abuse.
- Improved transparency and communication of protocols followed when reports of abuse are made, including average response times, so that reporting users are able to know the timescale for action with regards to when and if the problem will be dealt with and if and when the content will be removed.
- Increased moderation of user-generated content. This moderation is especially important where a service is proactively promoted and used by children.

- Prominent signposting to sources of expertise, advice, support and help for users affected by threats or abuse.
- A code of practice relating to anonymous use of sites.

21. We would also like to see service providers working more closely with the organisations dealing with the consequences and aftermath of online threats and abuse taking place through their services, providing both support and funding.

Real sanctions with statutory backing if necessary

22. Given the anonymity afforded online there can be a perception that abusive behaviour on social media is without consequence. We welcome the clarification from the CPS on this issue but we would like to see increased sanctions for abusive or threatening behaviour online which reflect those which exist offline and in other forms of media. For maximum efficacy we believe these need to have statutory backing.

September 2013

Written evidence submitted by South West Grid for Learning (SWGfL)

Summary: With over 10 years of pioneering work in online safety and as part of the UK Safer Internet Centre, we are fully aware of emerging technologies and potential risks, the issues children and young people, professionals and parents face, and the gaps that exist in their support; as well as stakeholders and partner organisations working in this field. In the response below we outline strategies we feel would improve online safety in the UK:

- **For point I. How best to protect minors from accessing adult content we recommend parent/filtering tools together with wide education campaigns, better content rating mechanisms and more research to identify gaps in support and provision.**
- **For point II. Filtering out CAI material we recommend providers should be members of IWF and the increased use of alert tools.**
- **For point III. Preventing abusive comments on social media we recommend a combination of prevention and empowerment strategies such as education and information about reporting abuse, and clear and simple reporting mechanisms from industry.**

1. Background to SWGfL:⁴⁸ Our esafety team of experts has national and international reputation in safeguarding children and young people online. Our expertise is around e-safety policy guidance and improvements and training in schools to staff, parents and pupils. We produce award winning resources such as 360 degree safe⁴⁹ used by over 4,000 schools to assess their esafety provision, pinpoint their weaknesses and make appropriate improvements. We also collaborated with OFSTED to inform the inspection of esafety standards in schools and early years settings.

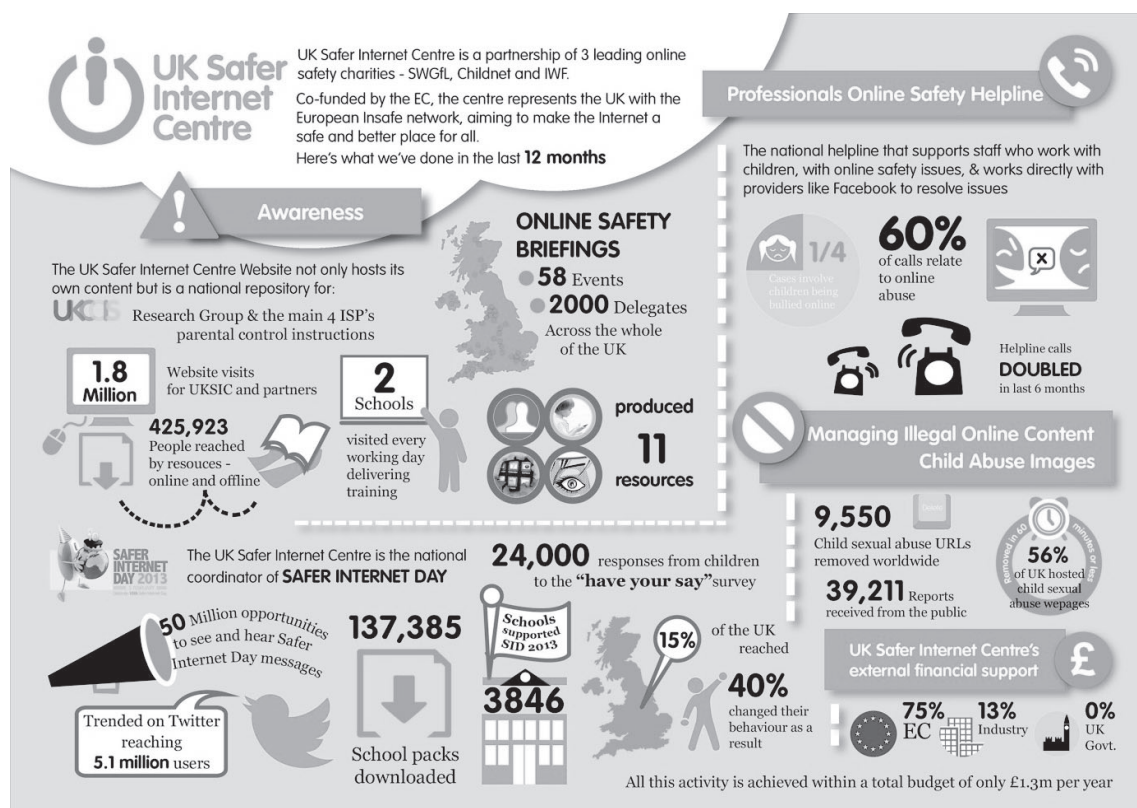
2. Role within UK Safer Internet Centre: As one of the three partners comprising the UK Safer Internet Centre,⁵⁰ SWGfL operates a unique helpline⁵¹ for professionals to help resolve online issues about themselves or the young people they work with. The centre also coordinates Safer Internet Day every February in the UK. To illustrate our work from the last 12 month here is an infographic:

⁴⁸ <http://www.swgfl.org.uk/Staying-Safe>

⁴⁹ <http://www.360safe.org.uk/>

⁵⁰ <http://www.saferinternet.org.uk/>

⁵¹ <http://www.saferinternet.org.uk/about/helpline>



1. How best to protect minors from accessing adult content

3. Adult content presents a range of harmful risks to children and young people and a number of strategies are required to best protect them. In this context, we are considering legal adult content. Children and young people have many influences on their lives- their age, social & economic environment, location, family situation, parental and peer groups etc; hence a single strategy is ineffectual. A broad complement of strategies would include:

4. **Filtering/parental controls:** There has been much discussion recently in relation to filtering or parental controls and whilst we support "Active Choice", we think that this is not a panacea. Parental controls have advantages to help prevent accidental access to adult content, however we know it will not prevent determined access, especially for "tech savvy" teenagers. Over the past 14 years we have been providing network level filtering into schools in South-West England and continue to see "loop holes" that children discover to circumvent and bypass the filtering in place. As we move towards multi device access in the home, our preference is for network level filters compared to device specific ones. We encourage parents to use parental controls and advocate age appropriate filtering, however always point out that these should not be used in isolation but alongside other strategies—filtering and parental controls are not a "fire and forget" solution. Consoles already use content ratings like PEGI and BBFC but these need to be more sophisticated on cable, TV services, mobile devices and app devices.

5. **Safe Search:** Linked to filtering, we encourage parents to use safe search functionality and age appropriate settings for online searches. It would be worth considering applying "active choice" to these services? For example safe search could be enabled as the "default" configuration, allowing users to "opt out" if they wish?

6. **Education for young people:** Education is the most important strategy. We should provide children with age appropriate, reflective, non-moralising and non-sensationalist educational programmes, mapped across the wider curriculum and covering the broader aspects of digital life, alongside parental support initiatives. Integrating discussions around sexting and impact of online pornography into RSE (Relationship & Sexual Education) is in our view the most suitable approach, ensuring that children understand the context around online adult content. Our fears relate to the influence of adult content on children's expectations and normal healthy sexual development. Whilst these are high level objectives, the effective success will require additional education and support for those raising these issues with children.

7. **Education for parents:** In our experience parents can often feel intimidated when discussing technology with their children and extending this to adult online content can exacerbate the situation. Many parents will not appreciate the extent and extremes of adult content online, well beyond the sort of content they witnessed as children. Support in this regard will be required, perhaps using a storyline in popular "soap operas" can help to raise the subject and allow parents to both progress discussions and to provide some messaging to children directly.

8. Education for teachers: Our evidence suggests that online safety training for teachers is consistently the weakest part of a school's wider online safety practice. The impact of adult content should be integrated into staff training and should extend to all staff. Pedagogical methods of integrating into RSE and online safety sessions should be provided to teaching staff.

9. Social Workers: Social workers (and social care professionals) who work with society's most vulnerable children should be able to access materials, resources and support in this regard. Combating CSE (Child Sexual Exploitation) is clearly a key priority in this sector and online adult content has a significant impact. Social workers should be able to recognise the impact of this content in particular cases.

10. Service Providers: For those service providers who do not allow or host adult content (as defined by the terms and conditions), they should be clear about how they monitor and enforce their policy, together with clear and transparent reporting procedures for users to report questionable content. For those service providers who do permit adult content, it should be clearly marked as such. Perhaps the use of age rating (ie 12, 15 and 18) could have a part to play? Providers who host user generated content should consider implementing user or community ratings.

11. Public Health: Public health campaigns should be considered to raise general awareness of online adult content, perhaps extending or integrating with existing teenage pregnancy campaigns, with which there is an obvious impact.

12. Research: Further research is needed to better understand the experiences, perceptions and knowledge of children and young people when it comes to online adult content together with assessments and evaluations of the impact of this variety of formal and informal educational programmes and resources.

II. Filtering out extremist material including CAI (Child Abuse Images) and material intended to promote terrorism and/or other acts of violence

13. IWF membership: UK ISPs should by mandatory requirement be members of the IWF (Internet Watch Foundation). Combating CAI in the UK through the work of the IWF has proved a particularly successful model and one that could be considered also for extremist material.

14. Using alert tools: SWGfL has been working with the IWF and South West police forces since 2006 to alert for any attempted access to websites containing CAI. This pilot project has been managed by CEOP with Home Office approval and due for evaluation shortly. The objective of the project is to flag intelligence to police forces if anyone in a school (specifically) attempts to access a website containing CAI. This intelligence prompts the police to then undertake their normal investigation routes resulting in a number of school staff, who have been identified and removed as a direct result of this simple alerting process. We believe we should use technology better to identify those accessing CAI (and extremist material) and we are involved in a project with Plymouth University and IWF to extend and refine our existing alerting capability.

III. Preventing abusive or threatening comments on social media

15. Background to Professionals Online Safety Helpline: The Professionals Online Safety Helpline, based at SWGfL is regularly called upon to comment on abusive online behaviours, both via printed and broadcast media and at public speaking events across the UK. The Helpline is part of the Safer Internet Centre, and is a dedicated service for professionals who work with children and young people, including teachers, social workers, police officers, youth workers, early years professionals and more. We have seen a large increase in calls from parents frustrated at the lack of practical help to get abusive comments removed online.

16. How the helpline operates: The helpline is unique in its approach to resolving social media issues, with a direct contact route in all of the major sites. Our current partners include Facebook, Twitter, Ask.FM, Instagram, Moshi Monsters, Tumblr, Apple, 192.com, Omegle, Snapchat and others. These contacts allow us in the first instance to ensure that the advice we give to callers about how to report, is accurate, and secondly, where necessary, to escalate the matter directly to the policy and safety personnel in each organisation, and have inappropriate, abusive content removed. In some cases this also leads to the perpetrator being suspended for their behaviour.

17. More guidance on how to report and remove content: Many services already exist to provide therapeutic support, particularly for children. What has been lacking is the practical guidance for users on reporting issues and ability to remove content. As such the helpline has addressed this gap and through its unique network of direct contacts to providers, supports professionals, and increasingly parents, in how to report abusive content appropriately in order to ensure or speed its removal.

18. Prevention strategies: Prevention is more challenging, and needs to be a collaboration between everyone involved. Schools, and even pre-school and early years settings, need to educate children about online behaviour much earlier. Generally where we see social media discussed and embedded in curriculum, there tend to be fewer issues and children take a more responsible approach. We believe children need to build a level of resilience, rather than being sheltered from experiences (of course we do not mean being subject to online abuse!). Schools should talk about how to respond to abuse, for example around blocking and reporting, and where possible introduce confidential reporting routes.

19. Strategies to empower young people and professionals: We know that children often do not “tell” when they are being bullied or abused. Allowing young people to report anonymously, either for themselves or their friends, can be very empowering. This can be simple, for example a “Whisper”⁵² alerting system via SMS, or email, or even a locked comments box. Other initiatives such as Anti Bullying Ambassadors also help discourage abusive behaviour. Schools need to act quickly and decisively when there are issues offline, often the online abuse follows a period of face to face bullying. If this is picked up earlier, better interventions can be put in place to support the child at risk.

20. Parental support: Parents need access to more up to date advice about specific popular sites, in how to support their child if the worst happens, and what they can expect from the child’s school. Schools need to alert parents of any bullying incidents at school as this can be an indicator that there may be issues online which the parent can assist with. Having regular, open conversations with their children about their online activities can help to identify potential risks before they happen, help children feel more able to discuss concerns, and also alert parents if their children are themselves engaging in bullying or abusive behaviours. Parents need to take a more proactive response when they discover their children are perpetrators of online abuse, including working with the school to ensure that they can support any victims who may not have already come forward.

21. Role of industry: Industry needs to ensure that they have sufficient safeguards in place to protect users. Our experience has been very varied, and some sites are better at dealing with issues than others. The most effective systems use a combination of automated systems, such as language filters (although these are in no way foolproof), automated moderation of specific phrases or search terms, and human moderation. It has been our experience that with very rapidly growing sites, including Twitter and Ask.FM, user safety isn’t considered as one of the priorities at the start. We are not overly critical of this, because having some flexibility around policy decisions allows for regular review and improvements to be implemented, however it can be dangerous to launch a site without some basic safeguards in place from the offset. An ideal approach would be a more proactive moderation, rather than a purely “report”-based moderation. We do not support censoring of the web, nonetheless making users aware that sites are monitoring behaviour may act as a deterrent for online abuse.

22. Clearer privacy settings and simple reporting routes: As well as working to prevent harassment, sites must adhere to their own community standards when reports are made to them. We would like to see much clearer advice on how to set up privacy on each site, report abuse, and clarification on what will happen once a report has been made, eg timescale for resolution. Reporting should be a very simple process, and we are pleased to see improvements to both Twitter and Ask.FM with the introduction of “in tweet” reports and a more prominent report button soon coming to Ask.FM. Matters must be resolved quickly, and with decisive sanctions, such as temporary suspension of accounts while investigations are underway. Our helpline is undertaking a national role of mediation with providers in reporting and removing abusive content and could be considered for national recognition like in New Zealand.

23. Accountability for anonymous services: We would also like to see more accountability to sites that allow anonymous questions, such as Little Gossip. Although most media stories would say otherwise, Ask.FM have been fairly proactive in dealing with cases reported to them, we have a named contact and they have kept us informed of policy and procedures. Little Gossip however do not respond to any requests for contact and act on abuse reports. This site allows users to report an abusive message by posting an equally abusive message in its place, leading to significant harm to the young people named and shamed on the site. We would like these sites to have an “opt in” to being anonymous, rather than “anonymous” being the default setting, and to have warning messages on their landing pages.

24. Support links and help: Sites should have better links to support services which are relevant to each country, for example Tumblr has links to self harm and suicide support services, but only in the US. Syndicated support would be more effective, where different providers point to consistent sources of support—for example to ChildLine, Samaritans etc.

25. Supporting organisations like the UK Safer Internet Centre: One area we would like improved is in financial support from industry to organisations such as the UK Safer Internet Centre, to produce resources and support operation of the Helpline, which directly tackles the issues users are facing. At present Industry contribute financially to the IWF in tackling child abuse images, but there is no co-ordinated approach to funding the services which resolve other problems such as removal of abusive content and in general, wider education and awareness-raising initiatives.

26. Role of Government: Government has an integral part to play, statutory funding should be in place for services working to resolve online harassment, and there needs to be clear direction and consistency between departments. Too often we are given conflicting areas of focus from the Department of Justice, DCMS, DfE, and even the Prime Minister. It would be more effective to streamline these through one distinct channel or Department. Government should also be more active and consistent in engaging with social media sites when there are issues in the public interest. There should be clearer guidance for the public on what legal action can be taken, and under what circumstances.

⁵² <http://boost.swgfl.org.uk/about.aspx>

27. **Role of media:** One area often overlooked is the responsibility that Media holds. While it's important to openly discuss online issues, we would like to see a more responsible use of language and reporting on behalf of the media. Often stories will have attention grabbing headlines, and very inflammatory language, for example "Facebook bully probe after death" and "How many more teenage girls will commit suicide because of Ask.fm". In nearly all the cases we have been involved in, media have made sweeping statements and assumptions about the circumstances of cases, without knowing the facts, and often while a Police investigation is still underway. These messages are very unhelpful, distressing for the families involved and some even contain inaccuracies about the sites which may lead to further problems. We would like to see the media adhering to a general code of conduct about how they respond to issues involving young people, and adopting more supportive safety advice and links to relevant resources.

28. **Users responsibility:** Finally, we need to consider the users themselves. In cases involving adults particularly, we need to be clear that if they break the law they may be prosecuted, that just as inappropriate offline behaviour may have legal consequences so may behaviour online. Young people's issues however are sometimes more complex, and we don't support criminalising children, however there does need to be a point when young people are held accountable for their behaviour. Awareness of those laws could be raised through an advertising campaign similar to TV licence/Road safety etc.

September 2013

Written evidence submitted by British Sky Broadcasting Limited ('Sky')

1. INTRODUCTION

1.1 We welcome the Committee's Inquiry into Online Safety as a further contribution to a topic that Sky has been heavily engaged in.

1.2 In June, we attended the summit chaired by the Secretary Of State for Culture Media and Sport, and have attached a letter we sent to her ahead of this summit as an appendix to this submission.

1.3 Over the last 20 years BSkyB has established itself as a successful and responsible consumer business. Since entering the broadband market in 2006, we have become the second largest provider in the UK with almost 5m broadband customers.

1.4 Our growth has come by providing customers with the products and services they want, and recognising the trust that our customers place in us to act responsibly. Over this time we have created a track record where we have helped families keep their children safe when enjoying the content we provide them on-screen and online.

1.5 The internet has become one of the most important sources of information, education and entertainment. Access to the internet is now an integral and fundamental part of people's lives, bringing with it a wide range of benefits but also a range of challenges.

1.6 There are many positive aspects to life in the online world, but just as in the offline world, there are services and websites that provide access to material that is not suitable for children. We have taken our philosophy of giving parents market leading tools to protect their families on screen, and applied it to our broadband services.

1.7 As a result, we have developed a range of tools to help parents manage how their families access content on whichever platform they choose to use, and are looking forward to enhancing our offering in the coming months.

1.8 There is a very important distinction to be made between content that is legal but potentially unsuitable for children, and other content which is illegal. It is vital that this distinction is not only understood by policymakers but highlighted at every opportunity to help ensure that there is more clarity in the debate, and in the way in which it is reported.

1.9 Sky's commitment to provide families with tools to choose how much of the internet gets through to their home, is separate to any legal or regulatory responsibilities we may have. Where content is deemed illegal by legislators or the Courts we will do everything required of us to prevent or restrict access.

2. PROTECTING MINORS FROM ACCESSING ADULT CONTENT

2.1 As a leading consumer brand, our customers have high expectations of Sky. They expect us to provide effective filtering products, presented clearly in an easily manageable way, which will enable parents to protect their families from legal, but potentially inappropriate content.

2.2 In addition to the work that we are doing to use technology to help parents, we believe that believe that industry, government and educators can work together to provide parents with the necessary information and advice to be able to make the most appropriate choices for their children, and to guide children and young people to make the right choices for themselves.

In home fixed line broadband

2.3 We offer all of our broadband customers free parental controls which are easily installed on customer's PCs or laptops. We use a category based web filtering package, which can be configured by age.

2.4 The internet is being accessed via an increasing number of connected devices including connected televisions, gaming consoles, tablets and smartphones. As internet use and the number of connected devices in customers' homes increase, so do the challenges for protecting families. Whilst the existing controls are an important tool for parents, as technology has developed, there is more that we are able to do.

2.5 We are in the process of developing an enhanced parental control product which will protect all the devices in customers' home. Whilst there remains a role for device manufacturers and operating system providers, we believe it is right for us to take responsibility and empower our customers to protect their families so they have confidence that the internet can be enjoyed in a safe environment.

2.6 Over the past few years, there have been policy questions as to the best way of delivering parental controls. Through our involvement in UK Council for Child Internet Safety we have engaged in Government initiatives such as the Bailey Review and the Department for Education's 2012 consultation, and the delivery of our new product is consistent with the features described in the Prime Minister's July speech on online safety.

2.7 Our enhanced parental control product will be free and available to all customers from the autumn. In addition to making the product available we are keen to encourage take up, and we will do this in a number of ways.

- I. From launch, when customers obtain new routers (by upgrading their router, moving to Sky Fibre or joining Sky as a new customer) they will be presented with the choice as to whether or not to implement our parental controls product. Furthermore, the "yes" button will be pre-ticked. This means that unless customers opt-out, and click "no", the customer journey will see parents install and configure parental controls to meet the requirements of their family. We have also introduced measures to ensure that an "age verified" adult is in control of the installation process and any subsequent amendments to the configuration of these controls.
- II. We will present all existing customers with a choice whether or not to apply the filters, and ensure that they have all made this decision by the end of 2014.
- III. We will support our new product with a major marketing campaign to encourage the adoption of the filters.
- IV. We are working with other ISPs and internet companies to highlight the importance of online safety, the use of parental controls, and to provide parents with more information on how they can protect their families in the online space. This will take the form of a major campaign launched early next year.

Out of home WiFi

2.8 Increasingly connectivity extends beyond the home. Sky's WiFi service, The Cloud, for example, provides customers with access to over 20,000 WiFi hotspots across Britain's High Streets, in venues such as Pizza Express and Greggs, and other public spaces like the London Overground railway stations.

2.9 When children are accessing the internet outside of the home, it is far more difficult for parents to monitor their activity, and our research tells us this is of concern to parents.

2.10 The Cloud pioneered offering its commercial customers the opportunity to automatically filter out access to adult websites in public WiFi hotspots, being the first WiFi provider to do so in 2007.

2.11 The increase in children accessing internet outside the home through connected devices, has led to parents seeking greater reassurance. That is why from September 2012, we decided to apply these filters by default, so that sites which contain content only suitable to adults are inaccessible in the public places served by The Cloud. As a leading WiFi provider, we think this is an important contribution to ensuring children are protected when using the internet outside of their homes, providing reassurance for parents.

3. ILLEGAL CONTENT

3.1 Separate from the issue of providing tools to customers to filter legal but potentially inappropriate content is our commitment to meet any obligations imposed on us to restrict access to content as a result of a legal determination.

3.2 Sky, as an ISP, is not in a position to judge the legality of a website or content within a website. Instead, Sky works with the bodies responsible for making such determinations and complies with any obligations it may have.

3.3 Content determined to be illegal tends to fall under one of three categories, namely child abuse imagery, material intended to promote terrorism and content infringing copyright.

Child abuse imagery

3.4 Sky is a member of the Internet Watch Foundation (“IWF”), which is the UK Hotline for reporting online child abuse imagery. Its key role is to get content removed at source. Where content is hosted in the UK, the IWF is typically able to get it removed in under an hour. Where content is hosted overseas, it takes longer to get it removed. However, the IWF provides its members with a list of URLs which contain illegal content. Sky ensures that requests to access such webpages, regardless of where they are hosted, result in a “splashpage” being served that informs the user that they attempted to access a page that contains illegal content.

3.5 Sky is a strong supporter of the IWF. We are currently engaging with the IWF to see how we can increase our support to it, both in terms of supporting the work they do and in terms of our financial support, where we are already part of the “top tier” of financial contributors. In particular, we are keen for the IWF to be proactive in seeking out illegal content rather than rely on public reporting.

3.6 It is worth noting that we have recently changed the splashpage served after requests from government and after consultation with the IWF, the Child Exploitation and Online Protection Centre (CEOP), and the Lucy Faithfull Foundation (LFF), which is a charity dedicated to reducing the risk of children being sexually abused. The splashpage now is more explicit in highlighting the consequences of viewing child abuse imagery linking to the LFF to provide further information.

Material intended to promote terrorism

3.7 We are keen to play our role in working with other Government departments, such as the Home Office, and its Counter Terrorism Internet Referral Unit (CTIRU) to ensure that illegal content is removed and/or filtered.

3.8 CTIRU was set up as part of the PREVENT strategy, to ensure unlawful online content is removed from the internet, thereby disrupting and limiting access to extremist material. Since its establishment in 2010, this unit has removed approximately 6,000 pieces of online terrorist content.

3.9 Sky does not provide webpage hosting, and as a result has not been requested to remove this type of content. However, we are keen to liaise with the government to explore whether there are other opportunities to work together.

Copyright infringement

3.10 Sky is keen to support rightsholders in seeking to restrict access to content that breaches copyright.

3.11 Although Sky is not in a position to determine which sites are making illegal content available, we welcome decisions by the Courts to require blocking of infringing sites, and have built systems to ensure we can comply with blocking requirements of resulting court orders.

3.12 We believe that the established process broadly works and has been accepted by our customers. Indeed, evidence from Ofcom’s research into online copyright infringement suggests a reduction in the people using infringing sites,⁵³ implying that blocking is a proportionate contribution to the fight against piracy.

September 2013

Written evidence submitted by Big Brother Watch

The Culture, Media and Sport Committee has decided to investigate a number of aspects of online safety that are currently raising concerns, in particular:

1. HOW BEST TO PROTECT MINORS FROM ACCESSING ADULT CONTENT

Firstly, it should be asked—is it the role of Government to prevent minors accessing adult content, or parents?

Critically—any measure must consider the privacy and freedom of speech issues involved. Given the importance of trying to help young people appreciate the importance of protecting their personal data and to consider what they are sharing online, intrusive “big sister” approaches should be resisted. If we raise young children with an expectation that they have no privacy, we cannot in later life then hope they discover the importance of privacy.

With nine in 10 parents aware that internet filters are freely available, it is clear that internet controls need to be made easier to use rather than taking the control away from parents and handing it to the government.

⁵³ http://stakeholders.ofcom.org.uk/binaries/research/telecoms-research/online-copyright/w4/OCI_MAIN_REPORT_W4_FINAL.pdf

“Thirty-two per cent of those who consumed any content illegally claimed to use “peer-to-peer” (P2P) services.....This was the lowest level seen during the 13 months of tracking (it was 37% in [the last set of research])”

The first problem associated with online safety is not only are there issues trying to define adult content, but there are differing views on what is unacceptable. For instance, some households would see topless photographs as adult content whereas others would not. This is why parental discretion is important. Opt-in filters remove parental discretion whilst risking some parents seeing all adult content as being impossible to access, therefore being less likely to discuss the issues that it raises. These are moral, not legal, judgements and parents are the only people who can make them.

Providing the choice for parents is key, and the Government has rightly pressed industry to make those choices available and easy to access. However, Government should not be seeking to tell parents what is the right choice and should absolutely have regard for what is technically feasible, particularly when trying to minimise circumvention.

We are concerned that the policy to date has been framed around the idea of creating a “safe” internet, and that once a filter is activated parents can relax. There is a real danger of lulling parents into a false sense of security, whilst simultaneously doing nothing to address the wider importance of education and discussion among families. Equally, the system does nothing to deal with situations where parents quite reasonably do wish to access legal content, but now feel trapped between a binary choice of “on or off”, neither of which works for them.

As a result, whether pornography websites or eating disorder discussion boards, deciding how to categorise the 2bn+ webpages now live is a gargantuan task, and given that nearly all the content is legal, creating a framework that is satisfactory to all is inevitably impossible.

Ultimately, any filtering risks driving content off-web and underground. From driving vulnerable people to more obscure sites where context is not provided to creating communities based upon the circulation of certain content, the essential part of child safety is dialogue with parents.

We believe that device level filtering would be a more preferable solution to network level filtering, and the Government by its approach has pushed the solution to a network level. Device-level filtering has several advantages. It allows granular access for different members of the family and is far harder to circumvent than a network filter. There is also the ability to add exceptions for legitimate sites that are blocked locally, or increase the level of filtering, putting parents in control of what their children can see. We would also argue that children are likely to seek parental input if they are concerned. As the EU Kids Online, September 2011 survey found, 70% of children feel parental input is helpful.

Parents are far more aware than has been claimed about the risks online and of the tools available to them. Some parents will choose to trust their children and discuss the associated issues with them, rather than installing filters. Others will use filters, and some may not allow their children to have a computer in their bedroom. These are parental choices and should remain so. Equally, some of the statistics presented to justify greater controls have been deeply flawed—for example the Advertising Standards Authority rebuked the Carphone Warehouse for its marketing around the Bemilo mobile phone service, while the figure claiming one in three 10 year olds have seen pornography online was based upon a single canvass of a secondary school in North London, by Psychologies Magazine.

Finally, we would highlight the risks of over-blocking, which do a great deal to undermine confidence in filters, while also jeopardising e-commerce. If people are unable to access health advice or support services, the knock-on effects could be significantly damaging. Equally, for businesses trading online, particularly SMEs, the impact of being blocked can be financially destructive. The instances of legitimate websites being blocked and taking many months to be un-blocked is something that should be given proper attention.

We agree more can be done in this area. We believe the four points of action are:

1. An industry funded single point of contact (website/helpline) with advice on how to download/install filters.
2. Parents should be educated so that they are aware what harmful content is on the internet and what to be aware off in terms of their children’s viewing—filters must not be presented as a perfect solution for a “safe” internet.
3. Far more needs to be done to educate children about the risks of using online services, in the same way as there are risks about being in public unsupervised or crossing the road. An approach that seeks to mitigate risk by eliminating any potential circumstances where a young person may be exposed to “harmful” content is no less dangerous than a parent who tells their child to only ever cross a road at traffic lights. It fails to recognise the nuance of life and creates an impossible standard of behaviour for young people to adhere to.
4. Industry should work towards including URL checkers as part of their offering, so people can check to see if their website is filtered and on what grounds. A minimum standard of redress should be guaranteed so that wrongly blocked sites and accessible as soon as possible.

2. FILTERING OUT EXTREMIST MATERIAL, INCLUDING IMAGES OF CHILD ABUSE AND MATERIAL INTENDED TO PROMOTE TERRORISM OR OTHER ACTS OF VIOLENCE

This question comes dangerously close to conflating illegal content with legal content.

A critical part of this policy area must be a clear, unambiguous statement that the fundamental basis for any content being filtered without the input of consumers is legality.

The IWF produces a list of URLs that meet a strict test of hosting child abuse images. Given no such organisation exists for material intended to promote terrorism or other acts of violence; it is unclear as to what process would be followed for this material. Given the political nature of some of this content, it would be unacceptable for Government to be making this decision without independent oversight.

Definition and dissemination in practice is not simple, and should require due process.

Fundamentally however filtering this content is not and should not be seen as the priority. If content is illegal then the primary focus should be to find who is hosting the content and to prosecute them, while also removing the content at source. Filtering must not become the norm simply because it is easier than pursuing multi-jurisdictional law enforcement action. (We would also highlight how this relates to the wider issues surrounding foreign policy and filtering, particularly where Government seeks to filter content based on decisions made without due process. Our own process will be copied in regimes less democratic than our own, whether on morality or public safety grounds.)

3. PREVENTING ABUSIVE OR THREATENING COMMENTS ON SOCIAL MEDIA

Abusive and threatening comments are not solely an online phenomenon and it is important to maintain a sense of proportion when dealing with these issues.

It is also important to note the intent of Parliament when passing legislation, particularly the Malicious Communication Act and s127 of the Communications Act 2003, neither of which were ever intended to be a catch-all for social media behaviour. Both were passed before Twitter or Facebook existed.

Online speech is still speech and should not be subject to harsher legal sanctions because it is made online. The criminal sanctions regime that exists offline is adequate to protect from incitement and assault.

As with off-line behaviour, preventing behaviour is only ever going to be a product of education and intervention by those with a direct relationship with a child, particularly parents.

A parent led approach can also be supplemented with an acknowledgement by social media companies of the threats and abusive language that can be used online.

Companies should have processes in place to respond to comments that constitute criminal behaviour, and this should be done where possible with the community online playing a role to establish acceptable standards of conduct, rather than top-down blocking or closing down accounts.

We believe that when public speech has been deemed to be offensive then this is best addressed through free, open and honest debate. Offensive content should not be addressed through prosecutions. In December 2012 the Crown Prosecution Service felt it necessary to publish interim guidelines for prosecutors on the approach to be taken in cases that involve communications or messages sent by social media. The guidelines outlines the need for communications to be “grossly offensive” or “obscene” for a prosecution to be made, however there remains an urgent need to reform laws that pose a serious risk to freedom of speech after several baffling prosecutions in the last few years. The legislation, on which these guidelines are based, was designed for a completely different purpose but now allows the CPS the right to police comments made on social media.

The danger is that while these guidelines may reduce the number of prosecutions, arrests will continue and only those with the stomach to take a case to court will escape without the long-term handicap of a criminal record by accepting a caution. Too frequently we are seeing people being offended on behalf of others and the legal system should not allow itself to be dictated by mob rule. Instead, the police should focus on bringing to justice those who seek irrefutable harm, rather than those who clearly seek to cause offence.

Equally, it is important that policy reflects the fact that both service providers and networks are not in any way the appropriate bodies to be deciding what is and is not acceptable speech—particularly given many of them will have users in countries around the world.

People, not technology, are responsible for how it is used and policy must respect the neutrality of networks and not try to turn them into an arm of enforcing a particular moral or legal framework.

Written evidence submitted by BT

BT welcomes the opportunity to provide written evidence to the inquiry.

KEY POINTS

- BT takes the issue of online child protection very seriously. We have long played an active role in trying to ensure that children and young adults can safely experience the many benefits of the internet. BT has invested over £5 million in tools and education since 2010 alone to ensure the UK is the safest online environment in the world for young people.
- BT has made substantive progress in supporting the Government's objective of providing family friendly internet services and continues to invest in our network and software whether in the home or public wi-fi networks. Active/unavoidable choice to install parental controls and not "default on" (where parental-control blocking is already applied and a user has to switch it off if it is not required) is better suited to engaging parents and driving awareness of the need to protect children online.
- It is not just about providing tools and gadgets—raising awareness of the need to protect children online and providing education on how to do so is crucial.
- Industry and Government have shown the potential of collaborating effectively on online child protection. A voluntary approach should be left to develop before considering any formal regulation or legislation.
- In the absence of clear primary legislation from Parliament, or an EU-wide legislative instrument, internet service providers (ISPs) should not be asked to police the internet beyond preventing access to illegal material such as child-abuse images.
- It is vital that ISPs receive clarity and comfort under the Regulation of Investigatory Powers Act (RIPA 2000) that their employees and/or those of their wi-fi site partners would not be at risk of a criminal prosecution related to the provision of network level content filtering services for blocking unsuitable content from reaching vulnerable individuals.

Further information will be found in our submission below.

BLOCKING ACCESS TO INAPPROPRIATE MATERIAL

1. BT blocks access for the following reasons, to:

- prevent access to illegal online child-abuse material, according to the Internet Watch Foundation (IWF) list. BT will automatically block any website that is on the IWF's list. This will be blocked for all BT customers, regardless of their connection. If a customer tries to access a web site that is blocked because it is in the IWF list, they will be redirected to a splash page.
- fulfil a customer request to block inappropriate online content, eg, if a BT broadband customer has opted into parental controls or a wi-fi site partner has decided that it wants wi-fi filters in its place of business.
- protect children in public places: providing BT Wi-fi's site customers with the ability to block pornographic material being viewed over the free wi-fi access provided in cafés, restaurants, shopping centres, etc.

BT TAKES ONLINE CHILD PROTECTION VERY SERIOUSLY AND HAS LONG PLAYED AN ACTIVE ROLE

2. In 1996, BT and other internet industry members came together to found the Internet Watch Foundation (IWF) of which we are a board member. BT then worked with the IWF to develop "Cleanfeed", the world's first system for blocking online child-abuse images. We have recently committed to increase our financial support of the IWF to enable it to proactively identify and remove illegal content from the internet.

3. BT has served as an active member of the Government's UK Council for Child Internet Safety (UKCCIS) since its inception in 2008. We are currently a board member and play a central role in developing the policies for online child safety for fixed and public wi-fi access. BT was also instrumental in developing the UK Government backed ISP Code of Practice, published in October 2011. This code outlined a set of core commitments for each of the UK's top four ISPs to inform and educate parents on content filtering tools available to them to enable a safer internet for their children and families.

4. BT has also played a key active role in the work initiated by Commissioner Kroes on the CEO Coalition initiative: "To make a better internet for kids," which has again shown the potential for industry and government to come together and collaborate effectively on child protection.

5. We have also been an active member of the Family Online Safety Institute (FOSI) since 2007. BT was instrumental in the launch of Childline 26 years ago and continues to be a strategic partner. We also work with partners such as The Parent Zone and the Child Exploitation & Operations Protection centre (CEOP) for reporting of online content. These arrangements work well and we continue to work with these partners, improving online safety for users and non-users.

6. Our customers have been offered free parental control software for years. Parents can block up to 35 categories of online content, everything from pornography through to suicide-promotion sites. Parents can also limit the time spent online by children every day; receive email and text alerts if children try to visit blocked sites or chat-rooms; control their use of social media and get reports on children's online activity. Different settings can be chosen for children of different ages, and the settings can be easily adjusted by parents.

7. BT also provides customers with information on safety, privacy and reporting on our bt.com website (see Annex 1), which also contains links to the IWF and CEOP. BT has developed a number of Acceptable Usage Policies (see Annex 1) that help customers benefit from safer surfing and minimise the risk of suffering online abuse.

BT CONTINUES TO INVEST IN NETWORK AND SOFTWARE SOLUTIONS AND HAS MADE SUBSTANTIVE PROGRESS IN ENSURING A FAMILY FRIENDLY INTERNET

8. The Bailey Review of the commercialisation and sexualisation of childhood in 2011 and the 2012 Government response to the DfE consultation both concluded that "default on" was not the right approach but rather active/unavoidable choice was better suited to engaging parents and driving awareness of the need to protect children online.

9. With this in mind, we have:

- launched active choice parental controls for devices in the home this year. This is free downloadable software which provides full protection and parental controls for a particular computer. These parental controls work for any internet connection and allow blocking of particular pages/content on a website, eg, certain YouTube clips can be blocked without restricting access to the whole website;
- pledged to provide all new and existing customers with an unavoidable choice to install network-based parental controls. By installing additional functionality within our network we are able to provide protection for all devices either at home or in UK BT Wi-fi hotspots;
- launched a pornography filtering solution, BT Wi-fi Protect, for our wi-fi site partners, eg, Starbucks in 2013 and writing to all customers to encourage them use it while applying by default blocking to all site partners where unsupervised children are reasonably expected to be present. To protect BT's consumer broadband customers who have access to BT Wi-fi's estate of c4.5 million public wireless hotspots, BT will extend the same filtering protection that BT customers receive from their home BT broadband following the roll out of our new network based home-filtering solution this year. Where a non-BT customer is accessing our hotspots, the vast majority purchase access via credit cards which effectively validates they are adults;
- launched the use of a "splash page" (the first ISP to do so) in place of an "error 404" message when users intentionally or accidentally access child abuse material that has been flagged by the IWF; and
- supported the development of industry-wide marketing campaign to drive awareness and education around online safety for children for launch in 2014.

RAISING AWARENESS AND EDUCATION IS CRUCIAL

10. BT believes that there is no substitute for parental engagement and diligence in monitoring children's use of the internet. To raise parental awareness of safety concerns and to provide education for protection against these, BT provides a range of helpful articles, videos and tools (see Annex 2). BT is also piloting our *Living with Technology* project where trained BT staff volunteers visit schools to help parents understand some of the key risks that children are exposed to on the internet and what tools and techniques are available to keep their children safe online.

11. Feedback from parents to date has been very positive as follows:

- 96% said they felt more confident about keeping themselves and their families safer online after the school workshop.
- 91% learnt something about keeping children safer online that they hadn't previously considered.
- 88% said they would discuss e-safety issues with their children.

ISPs SHOULD NOT BECOME ARBITER OF TASTE AND DECENCY FOR ONLINE CONTENT

12. In the absence of clear primary legislation from Parliament, or an EU-wide legislative instrument, BT does not wish to police the internet beyond preventing access to illegal material. To do so would set an unfortunate precedent in which an ISP would become the arbiter of taste and decency in relation to online content. It is not for an ISP to be placed in such a position.

RIPA 2000 CONCERNS

13. Legal opinion informs us that filtering any internet material on home broadband or public wi-fi may be illegal under RIPA 2000 and that this is so even if the purpose for filtering is child protection, and even if the internet user has chosen to set up filters. BT has raised with government the potential conflict between network-level content filtering and the Regulation of Investigatory Powers Act (RIPA 2000). We would expect to receive clarity that our employees and or those of our wi-fi site partners would not face a criminal prosecution under RIPA 2000 by offering filtering activities to our wi-fi site partners for blocking unsuitable content from reaching vulnerable individuals.

Industry Voluntary Approach

14. Industry and government (UK and EU) have shown the potential of collaborating effectively on online child protection. This voluntary approach should be left to develop before considering any formal regulation or legislation in this area.

CLEAR SET OF POLICIES FOR CONDUCT STANDARDS ACROSS BT'S SOCIAL MEDIA PRESENCES

15. BT's social media team has a very clear set of policies on conduct standards across our social media presences. On Facebook we have house-rules and we deploy a "swear filter" to hide the most offensive comments. On our BTCare⁵⁴ forums we publish Terms of Use & Guidance and we have an abuse report feature on the forums to allow members to alert us to violations. We also train all our social media advisors, forum moderators and managers on what they should do if they see behaviours which need moderation action. These include, but are not limited to, trolling, bullying, & spamming.

September 2013

Annex 1

BT'S ACCEPTABLE USE POLICY (AUP): INTRODUCTION SECTION

For the Internet to operate in a manner that satisfies the majority of its users, all users need to observe some rules and behaviours governing their use of it. These requirements are usually contained or referred to in the relevant terms and conditions governing the particular Internet service as well as the law.

To enable its customers to have a better understanding of what is and is not acceptable when using the Internet, and to help you get the best out of the Internet, BT has developed a number of Acceptable Usage Policies. These policies should help you benefit from safer surfing and minimise the risk of suffering "online abuse".

We have also included some general advice on how to protect you and your computer to each of these policies which we encourage you to follow.

ILLEGAL AND INAPPROPRIATE ACTIVITIES

As an Internet user, whilst connected to the Internet via BT you must comply with the relevant laws that apply in the UK. You should also be mindful of the fact that the Internet is a global medium and is regulated by the laws of many different countries. Material which is legal in this country may be illegal in another and vice versa.

These are some of the things that you must not do whilst connected to the Internet:

You must not, by using the service, download, possess or transmit in any way, illegal material (for example indecent images of children).

You must not send, publish, distribute, circulate or otherwise propagate any material that may be deemed to be grossly offensive or of an indecent, obscene nature or menacing in character.

You must not send, with the intention of causing annoyance, inconvenience or needless anxiety a message that you know to be false, or to cause such a message to be sent or to persistently make use of our service for that purpose.

You must not gain or attempt to gain unauthorised access to any computer systems for any purpose, including accessing the Internet.

You must not, without authorisation intentionally impair or attempt to impair the operation of any computer, prevent or hinder access to any program or data held in any computer or to impair the operation of any such program or the reliability of any such data (this could include deleting files, changing the desktop settings introducing viruses etc).

You must not infringe the rights of others, including the right of privacy and copyright (an example would be sharing without permission of the copyright owner protected material such as a music or video file).

⁵⁴ BTCare is a service brand in the social space which aims to drive customer loyalty by making it easy to get help they need.

Many of these activities could result in legal action, a fine or a term of imprisonment or both.

If you are in any doubt as to the legality of anything, take independent legal advice before proceeding.

BT'S OBLIGATIONS

BT is obliged under the Regulation of Investigatory Powers Act to disclose information to Law Enforcement Agencies and Public Authorities that are legally entitled to obtain such information. Similarly BT must comply with court orders to disclose information. In serious instances of abuse we may also notify the police or relevant law enforcement agency. BT cannot and does not monitor content of its' customers webspace or content of chat rooms, instant messaging, email, newsgroup or indeed of any communications and therefore BT cannot and does not guarantee that all of these are free of illegal material or other content considered unacceptable by others including the Internet community.

CHANGES TO THE ACCEPTABLE USE POLICIES

We may change the Acceptable Usage Policies' from time to time and will inform you on this website when we do so. To make the most of the guidance contained in the AUPs, please keep up to date with changes and look at them on a regular basis. We hope you will find them useful and informative.

BREACHES OF ACCEPTABLE USE POLICIES

Reports of breaches of these acceptable use policies by BT customers can be sent to abuse@bt.com.

BT may operate systems to ensure compliance with these acceptable use policies, including without limitation network scanning and testing of open servers and mail relays.

Annex 2

EXAMPLES OF BT'S EDUCATION AND AWARENESS ARTICLES, LEAFLETS, VIDEOS, TOOLS

Teens and social media

<http://home.bt.com/lifestyle/familyhome/parenting/teenagers-and-social-media-11363812320068>

Safe surfing for kids

<http://home.bt.com/lifestyle/familyhome/parenting/safe-surfing-for-kids-11363817423643>

Cyberbullying

http://home.bt.com/lifestyle/familyhome/backtoschool/cyberbullying-explained-11363834477238?s_cid=con_social_TW_portal

An article on online grooming is currently being created and will be live by the end of September 2013.

BT Family Protection parental controls

www.bt.com/familyprotection

A video to help customers set up Family Protection parental controls

http://bt.custhelp.com/app/answers/detail/a_id/13209/kw/family%20protction/c/346,2771,2774/session/L3RpbWUvMTM4MDEzMjA3MC9zaWQvcE9ET25jQmw%3D

Written evidence submitted by Russell Hopwood

- The concept of a criminal offence.
- Parental responsibility.
- Allowing access should be a criminal offence.
- Investment—no expense should be spared.
- The responsibility of Government, industry, parents, and children.

1. The CSM website states "it is a basic necessity the Children are safe from cruelty and harm no matter where they are, and that includes when they are on the internet".

I would comment about this that it is a criminal offence to inflict cruelty and harm on children by whatever means. This must include making available material which they can access whether it be online or in shops or any other source. I was involved in representation to my local MP about explicit material being on view to minors in newsagents and other shops. I may say I had his full sympathy with my concern. It is my observation that we are battling with certain media in this connection. Online purveyors of filth need to be held responsible just as the media do. The prevention of access to minors is like trying to bolt the gate when the horse is at least half out.

2. To reinforce this point it is clear that teenagers are very clever at accessing material online, and the figure of 81% of 14–16 year olds who do, illustrates this. However hard we try to restrict access, and I am not saying we shouldn't try, they will find ways of doing it. I am convinced much more needs to be done to prevent blatant filth being easily accessible. Having ten grandchildren myself, 15 and under, who have never accessed this sort of thing reinforces my belief that much comes down to parental protection and the environment the children are brought up in. It ought to be an offence for parents not to have filters in place, to say the very least. The principle of responsibility is a logical one in both these points.

3. The suggestion that we are restricting freedom of choice is as stated, a poor argument. It is an argument often heard in many areas of life. If I knew that there was a child-murderer in the neighbourhood I wouldn't propagate the argument that people should be free to leave their doors unlocked on the ground of liberty, or if the plague was spreading in my neighbourhood I wouldn't argue that people shouldn't protect their children from it. Is there any difference between this and the spurious right to allow access to damaging material. It is not a right at all, it should be an offence to allow it or to promote it.

4. I would fully support any investment that might be necessary to protect children online. I cannot comment on what is suitable, I would leave that to others. All I would say, is that whatever the cost it would be a good investment. If we want our youth to grow up as good upright honest young people, no expense should be spared. If we want them to grow up deceitful, devious, violent, corrupted in heart and mind, let the forces of evil have free rein. What is so appalling is that much of the harmful input is commercially driven. We need to get at the root as well as the branch.

5. One of the comments is "we believe much more needs to be done by Government, industry, parents and young people as well". Let us have a brief look at each of these.

Industry should take on the responsibility providing protection for young people. Let industry take on their share of the cost of protection, they can then roll the cost back to the paymasters whoever they may be—the sources of the evil material, the purveyors of it and the media. I am sure much more could be done to improve protection in terms of technological developments.

Government need to take on the responsibility of facilitating whatever legislation may be needed to enforce compliance. Let the politicians fully portray the horror of what is corrupting our youth. Let the legislators draft laws that will place the responsibility where it belongs. Let the Government see this as a battle against those who would undermine authority whether in the home or the schools.

Parents are primarily responsible for what comes into their homes and as suggested earlier should be held accountable for allowing access to harmful material. It is not intrusion into the privacy of the home any more than the need to investigate domestic violence would be.

Children become more responsible with age. As soon as they are old enough to distinguish between right and wrong they are to that extent responsible. Both parents and schools should be encouraged to promote a sense of responsibility. It could never be too young to do this.

Schools were not mentioned here, but I suggest we need a fresh look at what is taught in this connection. There are strong forces at work sweeping the western world to portray things as normal which arguably are the very opposite. The very least Government should do is give parents the right to opt out of lessons which they regard as weakening a healthy moral stance.

September 2013

Written evidence submitted by Stuart Taylor

FIRST: Congratulations, this is an excellent enquiry, and I wish and pray for your every success in it and that God may honour your endeavours.

WHO: (A) I write primarily as a parent/householder who has, with my wife, had the experience and responsibility of bringing up three sons and two daughters, seeking to teach them "*the good and right way*" (1 Sam 12 v 23) in view of marriage and the setting up of their own households.

(B) I also write as a Christian holding the Holy Scriptures as being the Word of God, affording all the guidance needed to protect our children. Isaiah 7 v 15 "*that he may know to refuse the evil and to choose the good.*" Romans 16 v 19 "*to be wise as to that which is good, and simple as to evil.*" 1 Tim 5 v 22 "*keep thyself pure.*" 2 Tim 2 v 22 "*but youthful lusts flee.*"

PARENTS: The prime responsibility to protect our children rests with the parents. We are responsible to care for them physically, morally and financially, and instruct them as to purity before marriage. Quoting the words of a Church Leader, "the greatest thing a man can do is to preserve his household [eg children]". Acts 16 v 31 "*Believe on the Lord Jesus and thou shalt be saved, thou and thy house.*"

Young people have naturally inquisitive minds and every possible effort should be taken to hinder the promotion of devices or circumstances which would leave them vulnerable or exposed.

As parents, along with other Christians, we set up our own schools in 1993 to endeavour to protect our children from the sadly declining activities and conversations amongst teenage children. We also supplied them

with computers which are limited and blocked from the defiling, corrupt and damaging materials which could normally be accessed. I know from bitter experience that contact with unclean literature can damage you for life. I personally know a Peer who always videos programmes before his children view them, taking out the harmful sections.

INDUSTRY: As employers, we would be selective of areas and buildings which we would work in and would personally be proactive in protection of our trainees and sub-contractors. The conditions of engagement include that no pornographic material or means of accessing it is taken on site.

GOVERNMENT: The government does have a responsibility to protect humanity and should be seen to be a terror to evil. Romans 13 v 3 *“For rulers are not a terror to a good work, but to an evil one.”* Filth is evil.

I would fully support that it should be mandatory for Government to impose strict sanctions where licensing for publications are granted with a penalty in place where these are not adhered to.

SUGGESTIONS: Your suggestion of default blocking facilities on all marketed internet devices is excellent.

The introduction of passwords or filters, such as declaration of age or a “general knowledge” question, the answer to which would be unlikely to be known by anyone under the age of 18, before access can be obtained is another suggestion.

Another possibility may be to link all licensed sites to national records such as registration of birth certificates/national insurance numbers/driving licence number, so that if a person’s details entered cannot be matched, access is denied.

Thank you for the opportunity of contributing to this enquiry.

September 2013

Written evidence submitted by Richard Browning

As a simple Christian, a believer on the Lord Jesus Christ, I submit this short piece to the Committee in a father’s and grandfather’s concern for the oncoming generations.

1. Essentially the young mind is inquisitive and constructive. This is witnessed not only in the human race but also in the animal creation; it is quite delightful to observe the tentative, halting attempts of the young hind or calf, rising to its feet, falling, stumbling, straining, tottering, until finally it leaves the ground and takes a few unsteady steps. With a child, development is very progressive; physically the watchful parents keep an eye open for anything that may hinder or stunt its growth, and is continually on the alert for danger, harm, unforeseen hazards.
2. This watchful care should be a lesson to us and should always mark the parent/child relationship. The child reaching maturity and finally having the privilege of caring for its parent would never forget the natural ties which existed; the experience always with the elder yet the strength in the younger.
3. I have little experience of the internet and of technology generally, but I regret the declining influence of a simple godly way of life, whilst acknowledging much good has arrived with the electronic age. I was always taught that the best way to distract a child and to save it from danger is to offer something else to draw its attention whilst removing the danger—such as a knife—at the same time.
4. The lack of respect for the nuclear family with its core of love and devotion between committed parents has resulted in fragmented and unequal households with little to attract and satisfy, and in undisciplined children. Government is partly responsible for this in its enactment of laws contrary to teaching in the Holy Scriptures.
5. It is incumbent on parents to be aware of where their children are as far as possible and not to neglect them selfishly. No home should contain “no go” areas where access is prevented and where harmful activities, literature and material can be hidden.
6. It is of course possible to obtain reputable computer security technology, to install it on all equipment in the household, to keep it up to date and to maintain firewalls and intrusion detection software. With virtually every household having internet access there is no easy fix. Much help can be obtained from websites such as “The Big 6 Online Issues”. Doubtless there are other sources.
7. Vigilance is required at all times in the protection of our families. Concerned parents will never surrender principles to expediency and for their own comfort turn a blind eye.
8. Read the Book of Job chapter 39, verses 14 to 16 “the ostrich which leaveth her eggs in the earth, and warmeth them in dust. And forgetteth that the foot may crush them, or that the wild beast may break them. She is hardened against her young ones, as though they were not hers; her labour is in vain without fear.”
9. May I respectfully request the Committee should be inspired by the teachings of Holy Scripture in the consideration of the inquiry; I am grateful for the opportunity to address it.

September 2013

Written evidence submitted by Timothy Michael Johnston

- I am very grateful to the Government for launching this inquiry regarding Online Safety. Having attended a number of debates in Parliament and studied the Press Reports over a number of years, I believe that this Inquiry is long overdue.
- Protection of children is at the heart of every parent and grandparent, and the advent of the internet and the simple accessibility of many websites by children and young people, is one of considerable concern.
- I thoroughly agree with the argument that access controls need to be installed on every computer in the UK, particularly to the websites providing entertainment.
- I believe that online gambling sites require age verification—surely therefore it is very simple to introduce the same filtering system where children and young people are seeking to access sites that are likely to harm them for life.
- The Prime Minister is to be congratulated on holding meetings with the leading ISP's, but he needs to be far more definite in insisting that these providers install these filters on their sites. I believe the Government are responsible to act very quickly on this issue—if there was an outbreak of war against Britain, the Government would step in to protect the people. The issue of online safety is a moral war on the safety and wellbeing of our youth and is the Government's prime responsibility to protect them. Without the introduction of stringent controls our future generations will be defiled, corrupted and harmed for life, which surely is the last thing that any right minded parent or grandparent would want.
- The complaint is often made that these sites originate from outside the UK—what is the difficulty in engaging the Governments on a global basis to combat this problem?
- I realise that this engagement is not a straight forward matter but if Britain doesn't take some strong measures against this avalanche of evil falling on our youth, then who is going to?
- I have listened to Members of Parliament strongly asserting the needs of these controls to be brought in to be put in place and I am most thankful to hear these sentiments.
- Could the CMS Committee ask the Government to set a timeline and target dates for the ISP's to introduce these filters? These companies are amassing millions in revenue every minute of every day from the internet, so it is not a question of the cost of introducing such filtering restraints, it is more the disposition or the mind to do it, and the Government should force this issue before we experience more and more tragedies.
- The recent horrific trials of persons murdering children surely galvanises this argument and make it very clear that something must be done and done quickly to protect our youth. Could the CMS Committee request the Government to set up without delay a legal team to look into the implications of introducing legislation to apply to the ISP providers in the UK?
- Could the CMS Committee invoke any current legislation from Europe to apply in this country, and if not, could this request be made to our European partners so any new initiative could be rolled out to all countries in Europe. At least this would ensure that there is some restraint introduced in this country and on the Continent.
- As a Christian parent and grand-parent, I would urge the CMS Committee to make a strong recommendation to the Government to introduce these filters with age verification as a matter of great urgency.

September 2013

Written evidence submitted by Lloyd Johnston

BACKGROUND

Having been born into a Christian household 30 years ago. I was brought up by my parents to live my life in accordance with the principles set out in the Bible. I have lived amongst Christians all my life and have proved times without number the benefits and protection of living with a sense of the guiding hand of God in my life.

DEVELOPMENTS IN INFORMATION TECHNOLOGY

Over the past century developments in communications and information technology have increased at an outstanding rate. There have been significant benefits to these developments in the business, political, education and many other sectors. However, there has also been with an alarming rate an increase in the exposure of risk to children. At one time there were only computers found in businesses, now if you asked most children of a reasonable age they would have in their pocket a phone of some type which would have access to the internet.

RISKS OF TODAY'S INFORMATION TECHNOLOGY

The access that the majority of children have to the internet is beneficial to them in many ways to assist them with their education etc. However, the risk that this poses at the current time is horrendous. There are two areas to which they are most vulnerable. The first is that they are exposed to any harmful contact online (eg grooming and sexting). The second is that they can easily access legal adult content that's not appropriate for their age.

Ofcom have stated that **81% of children aged 14–16 have viewed ADULT material online**. They have also found that **only 46% of parent have filters in place on their home internet**. Surely these two facts stand on their own, they give us a clear message that the status-quo is simply not acceptable. These risks cannot go on. Exposing a child to such filth could seduce their immature minds and change their characters for life. Such tools are being used in the world today to infiltrate, defile and corrupt the morals of simple people. A child with their inquisitive and curious mind may by total accident come across such material on the internet, they will instinctively click to look further and this one click is all it takes to scar, change the character and ruin that child's life. The youth today is being corrupted by the modern age. This has a knock on effect in the modern society where what was previously classed as unacceptable conduct is accepted now as normal. There are sadly in the world today evil persons seeking to attract children for filth through the electronic labyrinth of evil (the electronic systems of today).

I have been saved from my sins by the redeeming power of the precious blood of Jesus “who gave himself for our sins, so that he should deliver us out of the present evil world” (Galatians 1 v 4). I was once under the power of Satan “he who is called Devil and Satan, he who deceives the whole habitable world” (Revelation 12 v 9) but I am now saved for eternity. It is utterly abhorrent to me to think that we who live in a Christian country are allowing for such pollution to be available to young tender minds.

RESOLUTION TO THE UNPROTECTED ELECTRONIC AGE

It is with great appreciation I see that the Government are reviewing this whole issue. I fully support them in finding a resolution which will protect the young people and all residents of the United Kingdom from evil persons who would seek to harm them and from the adult material which is posted online.

There is one point I would fervently impress on the committee that they consider in reviewing suitable solutions. This is that any IT devices sold in the United Kingdom should have a standard setting on it which by default blocks all adult content on the internet. There should also be improved age-verification software installed on all devices.

I believe that some have tried to argue against suggestions such as I make above because of freedom of choice. We need to face the facts, 100 years ago such things as websites displaying this filth were not only not even thought about, and had they been they would have been outlawed immediately. Our previous generations then had no need for such material—why the change, can anyone justify to me why we need it now?

It is with greatest respect I submit this to the committee and will continue to pray that God in his infinite wisdom will give you the strength to stand for His rights, the protection of our nation's Christian values and the protection of the people (especially the vulnerable children) of the United Kingdom.

September 2013

Written evidence submitted by John Carruth

1. I take the liberty as a believer on our Lord Jesus, to express my concern to the committee regarding the ease with which the children of our nation are being corrupted by free access to online pornography. The results are alarming, the consequences unthinkable.

2. God in His word, the Bible, Romans 13 v 1–4 has set up government for the protection of its people. This present Government therefore has a direct duty and responsibility to urgently find a way to stop this poison being made available to our children. A complete ban would be excellent.

3. There is increasing genuine concern in this country about the control of this evil.

I would respectfully appeal to the committee to heed this concern and diligently pursue every avenue possible, to save the lives of our children.

September 2013

Written evidence submitted by Rob Barry

ONLINE SAFETY SUBMISSIONS

SUMMARY

1. Support for Current Online Safety Bill.
2. Biblical quotations.
3. Contemporary Quote.
4. Decline of Nations.
5. Extra suggestion.

ONLINE SAFETY BILL

1. I support the current Online Safety Bill 2012 promoted by Baroness Howe of Idlicote, or a similar provision to protect children from harm and inappropriate “so called” adult material. We need to help parents who can’t or won’t help themselves by providing the needed responsible legislation.

DRAINS AND SEWERS

In the same way that the Government provides drains and sewers for the physical health of the nation, they must provide for the moral health of our nation by containing filth and impurities.

2. **The Holy Bible containing Divine instruction** and sealed by the blood of Christian Martyrs contains the following Wisdom for mankind and Governments. (King James version). We do not have to be a member of a church to be responsible to God as Creator and to accept the special revelation from God in The Scriptures. We just have to be a member of the human race.

3. Timothy Chapter 3 v 16, 17

All scripture is given by inspiration of God and is profitable for doctrine, for reproof, for correction, for instruction in righteousness.

Genesis Chapter 2 v 15

*And the Lord God took the man [or Man] and put him into the garden of Eden to dress it and to keep it. [or “to till it **and guard it**” JND version]*

Romans Chapter 13 v 1—

*...the powers that be are ordained of God... v3 For rulers are not a terror to good works, but **to the evil**. ...v4 But if thou do that which is evil, be afraid; for he [the Government] beareth not the sword in vain; for he [the Government] is the minister of God, a revenger to **execute** wrath upon **him that doeth evil**.*

1 Corinthians Chapter 15 verse 33-

*Be not deceived: **evil communications** corrupt good manners.*

4. Timothy Chapter 2 v 17-

..their word will eat as doth a canker

*[or **their word will spread as a gangrene**]*

ANCIENT PROVERB

5. **“even evil words are dangerous”** “words that seem harmless because they float lightly like thistledown may bear in them a seed of evil which may take root and bring forth evil fruit”—an ancient proverb from Thais of Menander

(Rev Teignmouth Shore MA Canon of Worcester and Chaplain-in-Ordinary to the Queen 1897)

6. Decline of Nations

(a) Moral Decline or Degeneration

The condition of moral decline is seen as preceding with the decline in quality of life, as well as the decline of nations (Conservapedia.com)

An established morality is as necessary as good government to the welfare of society. Societies disintegrate from within more frequently than they are broken up by external pressures (Judge Devlin, Lawyer and Jurist 1905–92)

ETHICS/MORALS/VALUES/GOODNESS/OR RIGHTEOUSNESS

| | | |
|--------------------|-----------|---|
| Biblical Morality | 1800–1900 | Certain things are right and wrong and I know why |
| Abiblical Morality | 1900–1950 | Certain things are right and wrong but I don't know why |
| Immorality | 1960–1970 | Certain things are right and wrong but I don't care Sadly promulgated by The Beatle era through allurement of music |
| Amorality | 1970— | There is no such thing as right or wrong |

(from Allen Turner.com)

(b) *Rome*

Over five centuries the ancient Roman Empire spread to include an area from the Atlantic to the Euphrates, and England to the Sahara, until it succumbed to the Four Danger Zones of Morality (Smith 286)

Wealth, Force, Sex and Speech
(Affluence—Riches—Greed)

The needs of online safety can be mirrored in the decline of moral standards through the media, which in Roman times was the violence of the Gladiatorial combat which was essentially murder. Rome couldn't eventually fill its military ranks and the decadent civilians could not mount any sort of effective defence. The Theodosian Code eventually displayed an emotional confusion between sin and crime that would have been alien to the classical Roman law (159). When a nation possesses everything it needs and more, it becomes myopic, short sighted and no longer plans ahead to prolong the life of the nation. We cannot afford to be a showcase of smugness and apathy.

In 1993 the average American child had watched 8,000 televised murders and 10,000 acts of violence before finishing elementary school (American Psychological Association).

(Novelguide)

7. Suggestion

Have an x rating for certain sites that have to pay a taxation fee, if they cannot be removed altogether.

September 2013

Written evidence submitted by Barry Saltmarsh

I would like to express my views on this topic of the very much needed move to protect minors from accessing internet sites with adult content, which could cause a warping of the mind to the individual, in particular those who are young and impressionable, and who are the "Us" of tomorrow.

As a Christian and a believer on the Lord Jesus I find it abhorable that anyone should be linked, or have anything to do with to such adult sites, and would like to support those who would try to bring about a level of control to protect today's youth.

Surely with the technology available today there is an easy way to prevent minors from accessing adult content online.

Filtering out material such as child abuse and pornographic material would be a very welcome step, I would suggest default blocking of all adult material which would require authorisation to activate, as a standard setting on all internet devices sold in the UK.

This would provide a measure of safely to our young people, whom we are responsible for. As it speaks in the Bible, The Lord says "But whoso shall offend one of these little ones which believe in me, it were better for him that a millstone were hanged about his neck, and that he were drowned in the depth of the sea." Matthew 18:6.

This would show the depth of feeling the Lord Jesus has for children.

As a Christian nation we should bear in mind what we stand for, the ways and the life of Christ.

One welcomes the CO-OP's decision, mentioned in the *Telegraph* on Monday 9 September 2013, to remove unpackaged adult newspapers and magazines from their shelves to help to make their stores more family and children friendly; I look forward to many more retailers following suit. Why should innocent persons be confronted with indecent images whilst trying to lead a normal and respectable life style?

It is on us all, individually and as a whole to recognise the need of protection for our young people.

Whilst the internet has many benefits and is an incredible tool, we would have to acknowledge it also has pitfalls and traps into which the innocent can fall. Internet chat rooms also need some form of monitoring, to

try to minimise the possibility of young people being snared by paedophiles and murderers. One does not have to look far to read of situations where every parent's worst nightmare has come true.

Whilst any move forward is better than none, I believe there needs to be a purge of all such pornography and other suchlike material online and am greatly encouraged by David Cameron's move to ask the internet search providers to look into an element of control on this.

For the good of the nation as a whole can we join in in support to help to protect our children and future generations and help control what indecent material minors have access to?

I would like to point out two passages of Scripture which I feel fit in well with the whole issue.

The Lord said "Ye have heard that it was said by them of old time, thou shalt not commit adultery: But I say unto you, that whosoever looketh on a woman to lust after her hath committed adultery with her already in his heart." Matthew chapter 5, verses 27&28.

"For without are dogs, and sorcerers, and whoremongers, and murderers, and idolaters, and whosoever loveth and maketh a lie." Revelation chapter 22 verse 15.

To all who believe on the Lord Jesus and know that every word in the Bible is true, there can be no ignoring these words. A solemn warning to all, that there will be, in the in the day of judgement, a just and right God who will judge us according to our pathway in this world.

In the book of the Acts of the Apostles, chapter 2 verse 21 it reads "and it shall come to pass, that whosoever shall call on the name of the lord shall be saved", let us therefore rally together to find a way to try to rid, or at least limit the evil that there is available at the click of a button.

September 2013

Written evidence submitted by Safermedia

SHORT SUMMARY

1. How best to protect minors from accessing adult content:

- Opt-in ISP level filters are best, with customers given an unavoidable choice whether to apply them or not. Free public Wifi should all be filtered as standard (*I am not mentioning places where "kids don't go"*). Parents need more support to apply filters and talk to their children. Sex education in schools must not include (overly-delete) explicit material. Extensive research shows serious harm from pornography.

2. Filtering out extremist material, including images of child abuse and material intended to promote terrorism or other acts of violence:

- Government and especially industry must put far more funding into R and D.

3. Preventing abusive or threatening comments on social media:

- More R & D also needed here—to continue to develop and implement effective safety measures—inline with any other environment that is potentially dangerous for children. Robust and effective law enforcement is necessary.

4. Conclusion:

- Where a conflict arises the protection of children must always take priority over freedom of expression and commercial interests.

1. HOW BEST TO PROTECT MINORS FROM ACCESSING ADULT CONTENT

Filters

The vast majority of experts and childcare experts, including major children's charities, agree that ISP level filters with a default of porn off, and an "opt-in" for over 18s who wish to access all content, are currently the best way to protect minors. What was announced by the Primer Minister in July was slightly different (all customers will be presented with an unavoidable choice to apply filters or not) but we applaud his work to have this introduced for all customers of the big six ISPs by the end of 2014. However all ISPs should be included as soon as possible, and the system will only work properly if there is strict age verification. Close monitoring is vital. Ofcom, given this task by the Prime Minister, must without delay develop clear standards, with which all ISPs should be required to comply. Ongoing monitoring will also be key.

Recent research from the magazine PC Pro (Sept 2013) shows that 80% of parental controls fail to filter explicit material, with only three out of five of the most popular website filters being 100% effective in blocking pornography. This is an egregious situation for parents and carers and demonstrates clearly the need for automatic ISP level filters.

ISP level filters should apply to all internet-enabled devices including:

- (i) mobile phones. All 3G networks offer content filtering and it works well enough. However Voda, EE and O2 all let VPNs and proxy servers through, so if you know how, you can bypass the filters.

Vodafone and EE (tested by our technical adviser) do not enable Google safe search and so a simple search for obvious keywords and clicking on images yields lots of images. But usually if you click on one to go to the website, the content blocker will block it. This is something Google really needs to do more work on.

Figures suggest 91% of pre-teens and teens who have a smartphone have internet access 24/7. The pornography industry's main target is the 12–17 age group and they are putting huge efforts into monetising the mobile phone. Between 22 and 25 September the pornography industry XBiz conference was held at the Radisson Hotel in Bloomsbury in London and their focus **was on opposing UK plans to limit access to online pornography in the UK** <http://www.xbiz.com/news/168143>.

- (ii) public Wifi. Free public Wifi is used by many young people as it saves their own allocated usage and they can access content without their parents' knowledge if they wish. It was supposed to have been filtered by the end of August, but research this week shows that more than half of free public Wi-Fi networks let users access porn, violence and drugs. Mobile security firm AdaptiveMobile, tested the web filters on public networks across the country and discovered one in three UK cafes and restaurants have no filtering in place at all—leaving children in danger of accessing pornography.

The Government will clearly have to work much more closely with the industry and all who offer public Wifi to ensure progress is made in line with the Prime Minister's timetable.

Education

Parents are the most important people to reach with education about computers: they need to learn how to set up safety measures; to have an understanding of what children can and are doing online; to know how best to communicate with their children about internet use, and measures to protect their children. They must also be encouraged to talk a great deal more to their children about these issues and be helped with the skills needed.

Here also the Prime Minister has promised to make much more use of government resources to raise awareness among parents and empower them, and we welcome that.

Children need education too, but it must be remembered that teens' neural chemistry and reward signals means they are inclined towards risk taking and impulsive behaviour. Their natural curiosity and desire for independence can make them forget education and warnings by parents and other adults.

School

Although it would be helpful for schools to explain the dangers of online porn to children, we do not believe that there should be a change to the curriculum of SRE lessons as has been suggested by some. Teachers must also be very careful not to cover such explicit material that they themselves inadvertently introduce young people to porn. Again, it is extremely important for parents to be made aware so they can better protect their children and this could be done through courses in schools for example.

Other measures

Safermedia applauds the recent announcement that Government proposals include Banks and credit card companies blocking payment to websites with pornographic material.

Research showing serious harm from pornography

Finally it is very important to remember exactly why we need to protect children from adult content. The following examples give an idea of the large body of compelling international evidence showing serious damage to sexual development and behaviour from pornography:

- A. The Sexual Trauma and Psychological Programme, University of Pennsylvania:

"Overall the body of research on pornography reveals ... it functions as a teacher, permission-giver, and a trigger of ... negative behaviours and attitudes. The damage is seen in men, women and children, and to both married and single adults ... pathological behaviours, illegal behaviours and some behaviours that are both illegal and pathological."

This research forms part of "The Social Costs of Pornography: A Statement of Findings and Recommendations," the findings of an inquiry and consultation that ran from 2010–12, sponsored by the Witherspoon Institute and the Institute for the Psychological Sciences. Fifty four of the ablest professionals and academics in law, medicine, political theory, philosophy, religious studies, history and several other disciplines contributed.

- B. "A meta-analysis of the published research on the effects of pornography," Elizabeth Oddone-Paolucci, Mark Genuis and Claudio Violato, University of Calgary. Medicine, Mind and

Adolescence, 1997. The 46 studies (from 1965 to 1995) included 12,323 people. *“The results are clear and consistent; exposure to pornographic material puts one at an increased risk for developing sexually deviant tendencies, committing sexual offences, experiencing difficulties in one’s intimate relationships, and accepting the rape myth. In order to promote a healthy and stable society, it is time that we attend to the culmination of sound empirical research. The rise in sexual crimes, sexual dysfunction and family breakdown may be linked to increased availability and use of porn.”*

May we point out that these are both extremely extensive pieces of work, the former being a multifaceted, multidisciplinary and scholarly exploration of the issue, and the latter a meta-analysis of previous research.

- C. Brain scan images of porn addicts show that watching online “adult” sites can alter our grey matter, which may lead to a change in sexual tastes. New research by Cambridge University neuropsychiatrist Dr Valerie Voon shows that men who say they are addicted to porn ... develop changes in the same area as heroin addicts—the reward centre—that changes in drug addicts. (Norman Doidge, The Guardian 26 Sept 2013)
- D. That so many children and young people are already manifesting serious effects from their easy access to pornography and other harmful content is reason enough for Government action to take on a sense of urgency (London Portman Clinic is one source).

2. FILTERING OUT EXTREMIST MATERIAL, INCLUDING IMAGES OF CHILD ABUSE AND MATERIAL INTENDED TO PROMOTE TERRORISM OR OTHER ACTS OF VIOLENCE

Adequate resources must be provided and used by search engines and ISPs to filter out harmful material which can be accessed via their platforms.

Adequate funding and resources provided by both the industry and Government to ensure those involved in investigating and removing such material could be very effective.

3. PREVENTING ABUSIVE OR THREATENING COMMENTS ON SOCIAL MEDIA

Safermedia wants to see Facebook and other social networking sites behaving responsibly and putting the well-being of children and other vulnerable groups first. Currently underage children are able to access social media too easily; 7.5m children under 13 have a Facebook page. Sites such as Tumblr have plenty of pornography; Facebook content can be pornographic; violently sexist and racist. It can poke fun at victims of terrorism, disease, etc. Much of it is inappropriate for 13–17s let alone under 13s. Social media (including chat rooms popular with young teens, etc) is also used by sex traffickers and paedophiles to groom children, and by prostitutes to solicit.

- Facebook’s own rules should better reflect the law in other forms of media. The making of rules by an operator who is making large sums of money from its users through advertising is not a satisfactory situation, especially where children are concerned.
- There needs to be improved moderating of these sites with proper training and compliance.
- There should be swift action to remove content when a complaint is received. This is a health and safety issue and other industries have to comply with strict regulation.
- Social media make vast amounts of money from the marketing and tracking of their users. They should have to take into account that children are immature and lack the judgment needed to make decisions about sharing their personal information online or to grasp the consequences of their actions on others.
- Urgent research and development should be done by industry to prevent inappropriate content being shared peer to peer.
- Robust age verification is vital if ISP filters and social media sites, are to protect children effectively.

Recent decisions by Ask fm and Twitter following public outcry have led to some improvements in safety measures. This is welcome and shows that the industry can and must do more.

4. CONCLUSION

Safermedia understands that immense benefits can be provided by unimpeded communication and free speech, and any attempts to mitigate harms have to be proportionate and, where possible, avoid disadvantageous consequences. However in a civilised democratic society the protection of the vulnerable must be at the top of the Government’s agenda, and our children fall into that special category, which must be above ruthless and exploitative commercial interests. There is not merely a moral but also a public health aspect to this—if the health, development and relationships of our youth are allowed to be undermined by harmful internet content, the whole of our society will pay: higher welfare and healthcare costs, more anti-social and criminal behaviour

and ultimately higher taxes for all of us. We trust that this Culture, Media and Sport Committee Inquiry will result in making the protection of our children and the stability of our whole society a top priority.

September 2013

Written evidence submitted by John Reiner

- Online dangers to children and young people.
- Current situation is unsatisfactory.
- Measures the Government could implement to increase protection.

1. I would like to emphasise the current dangers to children and young people using the Internet. The first concern is the possible exposure of children to harmful contact online (eg grooming and sexting). The second concern is the danger of young eyes viewing legal adult content inappropriate to their age.

2. Two key facts from Ofgem clearly demonstrate why more protection is required—a) 81% of children aged 14 to 16 have viewed adult material online, b) only 46% of parents have filters in place on their home internet. More needs to be done at Government level to implement blocking of unsuitable material.

3. Policy changes and investment of resources are required to increase the levels of protection provided for children and young people using the internet. Some specific suggestions I would like to make are: a) implementation of default blocking of all adult content to be the standard setting on all internet enabled devices sold in the UK to stop children from seeing adult content that could be harmful, b) the development and use of better age verification software. It is a basic necessity that children are safe from cruelty and harm. Measures like those suggested above are often watered down in the name of freedom of choice. This is a poor argument where the protection of children is concerned and should be resisted.

September 2013

Written evidence submitted by the Family Online Safety Institute

EXECUTIVE SUMMARY

- The Family Online Safety Institute (FOSI) submits these comments to the Commons Select Committee on Culture, Media and Sport to inform and educate the Committee as to the nature of the online environment in which children and families are currently operating, and the approaches being used to ensure that interactions on the Internet are being kept as safe as possible. Ultimately, opportunities created by the Internet far outweigh the risks that may be encountered online, and children can be taught to embrace the benefits of the Internet whilst learning about protecting their privacy and staying safe online.
- FOSI is working to create an online culture of responsibility that encourages governments, law enforcement agencies, industry, parents, teachers and children to work together to make the online world safer. Through this work, founded in research and with the benefit of international policy expertise, FOSI and its member companies are working together to develop best practices to help keep kids safe online.
- Teaching children how to embrace their rights and responsibilities whilst online will help to minimise risks and maximise the benefits of the Internet. The government can aid this process by funding research into online behaviours, prioritising digital literacy in the classroom, and informing parents of both risks and opportunities online. The continued collaboration between industry, teachers and the government to build these messages will ultimately empower parents to use existing tools, establish household rules and engage in a conversation to create digital citizens capable of navigating the online world safely, privately and in their own best interest.

SUBMISSION OF THE FAMILY ONLINE SAFETY INSTITUTE

1. The Family Online Safety Institute (FOSI) is pleased to offer this submission to the Commons Select Committee on Culture, Media and Sport. It is our hope that these comments will provide the Committee with clarity about the online environment that children are currently experiencing, as well as further insight into their behaviours on the Internet. The submission also aims to highlight collaborative approaches that can help to ensure online safety.

2. FOSI is an international, non-profit membership organisation⁵⁵ working to make the online world a safer place for children and their families. We do this by identifying and promoting the best practices, tools and methods in the field of online safety and privacy that also respect free speech. FOSI convenes leaders in industry, government and the non-profit sectors to collaborate and innovate new solutions and policies in the

⁵⁵ For more information see <http://www.fosi.org>. FOSI members include: Amazon, AOL, AT&T, BAE Systems, Detica, BT Retail, Comcast, Cyber Guardian, Disney, Eclipse, Entertainment Software Association, Facebook, France Telecom, Google, GSM Association, LinkedIn, Microsoft, Mind Candy, Motion Picture Association of America, NCTA, Nominum, Sprint, Symantec, Telecom Italia, Telstra, T-Mobile, The Wireless Foundation, Trend Micro, Verizon, Vodafone and Yahoo.

field of online safety. Through research, resources, events and special projects, FOSI promotes a culture of responsibility online and encourages a sense of digital citizenship for all. With roundtables, forums and conferences around the globe, FOSI plays an important role in driving the international debate.

3. FOSI achieves this aim in a number of ways. Firstly, through engagement with policymakers around the world. In the United Kingdom, FOSI has long been an active member of the UK Council on Child Internet Safety (UKCCIS) and now sits on the executive board. Since the inception of the European Commission's CEO Coalition to Make the Internet a Better Place for Kids, FOSI has had a high level of participation. In the United States, FOSI regularly engages at the federal and state level to provide resources and raise awareness about online safety efforts.

4. Secondly, FOSI achieves this aim through events. FOSI holds premier, highly visible conferences and forums around the world each year. We convene government leaders, industry members, teachers, parents, law enforcement professionals and charities to discuss and collaborate on finding actionable solutions to the challenges presented by the Internet. Whilst at the same time working to highlight what can be done to responsibly take advantage of the infinite opportunities.

5. Thirdly, FOSI has developed comprehensive, user-friendly resources for professionals and consumers. For professionals, we provide the Global Resource and Information Directory (GRID).⁵⁶ GRID aggregates online safety laws, education initiatives, research and active parties in over 190 countries, and is monitored by an editorial team to ensure accuracy after notable events or legislative shifts. Additionally, FOSI has developed a resource for parents, teachers and teenagers, called A Platform for Good,⁵⁷ which is designed to allow users to "Connect, Share and Do Good" online. It provides examples for teachers on how to incorporate technology into the classroom and gives children the opportunity to share stories on ways that they have used the Internet to help others or to enhance their own learning. Most importantly, A Platform for Good gives parents suggestions on how to talk to their children about staying safe online and provides interactive features and robust resources to help empower parents to become more engaged with the online lives of their children.

6. Finally, FOSI has conducted numerous research studies in the United States into the online behaviour of teenagers and the concerns of parents. Our initial effort looked at the use of parental control tools,⁵⁸ the second examined online behaviours and digital citizenship,⁵⁹ and the third explored the varied attitudes towards online safety between the generations.⁶⁰

7. In July 2011, FOSI and Hart Research Associates looked at the ways in which parents chose to monitor what their children were doing online and examined the awareness and use of technical parental control tools.⁶¹ Online safety remained an area where parents did not feel that their child was in danger, with 86% of parents reporting that they felt that their child was "very" or "somewhat" safe online. The proportion of parents who felt that their child is "very safe" decreased notably as the child grew older and spent more time online.

8. Findings showed that virtually all parents claimed to have talked to their children about their online behaviour and the associated risks and benefits, but just over half of parents say they have used technological parental controls for Internet use. Amongst those parents who did not use parental controls, the most oft-cited reason was that they felt that they were unnecessary, owing to household rules or because they trusted their child to act safely and responsibly online. Nearly all (93%) parents said they had set rules or limits in one or more ways to safeguard their children online.

9. Notably, parents felt more knowledgeable about how to protect their children's safety and privacy online when using a computer, as compared to smartphones or other handheld devices. Due to the constant increase in the use of mobile devices, this is an area in which more education and awareness raising should be encouraged. In response to these findings, FOSI created online safety contracts and other materials to help parents establish household rules and talk to their kids about setting limits for the sites they visit, amount of time they can spend online, and how they manage new devices.⁶²

10. Also in 2011, FOSI and Pew Research Center examined online behaviour and the notion of digital citizenship.⁶³ The research showed, unsurprisingly, that social media had become pervasive in the lives of American teenagers. 95% of those surveyed were online, and of that 80% were social media users. The majority of teenagers using these services reported that their peers were largely kind to each other on these sites. However, 88% of users had witnessed other users being mean or cruel on social network sites, yet only 15% of teenage social media users had experienced such harassment themselves in the past 12 months.

⁵⁶ For more information see <http://www.fosigrid.org>

⁵⁷ For more information see <http://www.aplatformforgood.org>

⁵⁸ 2011, FOSI, Hart Research Associates. "Who Needs Parental Controls? A Survey Of Awareness, Attitudes, And Use Of Online Parental Controls." http://www.fosi.org/images/stories/research/fosi_hart_survey-report.pdf

⁵⁹ 2011, Pew Research Center, FOSI, Cable in the Classroom. "Teens, Kindness and Cruelty on Social Network Sites: How American teens navigate the new world of 'digital citizenship'" <http://pewinternet.org/Reports/2011/Teens-and-social-media.aspx>

⁶⁰ 2012, FOSI, Hart Research Associates. "The Online Generation Gap: Contrasting attitudes and behaviours of parents and teens." <http://www.fosi.org/images/stories/research/hartreport-onlinegap-final.pdf>

⁶¹ *Ibid.* 5

⁶² See <http://www.aplatformforgood.org>

⁶³ *Ibid.* 6

11. Encouragingly, minors reported more positive personal outcomes than negative ones from interactions on social network sites: 78% report at least one good outcome, 65% had had an experience on a social network that made them feel good about themselves and 58% felt closer to another person because of an experience on a social networking site.

12. 95% of social media-using teenagers who had witnessed cruel behaviour on the sites say they had seen others ignoring the mean behaviour, but 84% had seen people defend the person being bullied. Children continued to rely heavily on parents and peers for advice about online behaviour and coping with challenging experiences.

13. The Online Generation Gap study,⁶⁴ undertaken in 2012, compared the attitudes and behaviours of parents and children with respect to online safety. There was a stark difference between the amount of knowledge that parents had about their children's activities on the Internet, and the realities of what their children were actually doing. However, both teenagers and parents felt that they were generally safe online, and, importantly, minors exhibited an awareness of their digital reputation, with over 80% having actively adjusted their privacy settings. Of concern was the statistic that 43% of teenagers admitted to posting something online that they later came to regret, a fact that emphasises the importance of education around privacy and reputation management.

14. It is essential to have an understanding of the environment in which children operate in order to create new initiatives and policies to enhance online safety and privacy. For now, it is hoped that the research findings, in conjunction with FOSI's international expertise and policy knowledge, will provide the Committee with a constructive context to their inquiry.

15. The Internet enhances the educational and social lives of children in the United Kingdom and around the world. Their use of media permits them to gain knowledge in a variety of new and engaging ways. Children are able to create and share their own content and express their ideas, thoughts and experiences on a worldwide platform. The Internet allows experiences that go far beyond their homes and communities; they are able to explore the world, immerse themselves in different cultures, geographies and periods in history instantaneously. The skills children learn through their online exploration in early life prepare them for their future and provide knowledge as well as the digital abilities that are vital for functioning in the modern technology-driven world.

16. The accompanying risks and challenges that go along with living in an online world can not be discounted. Often, the skills and knowledge children have about new media far exceeds that of their parents. There is illegal activity online, just as there is offline, and there is a possibility that children can be exposed to content and actions that are harmful to their development and well-being.

17. Consequently, at FOSI, we believe the key to keeping children safe and ensuring that they have safe, productive and private experiences on the Internet, is to build a culture of responsibility online. This can only be accomplished if six separate entities work together to create a safer Internet. The key components are: 1) government; 2) industry; 3) parents; 4) law enforcement; 5) teachers; and 6) children.

18. Reasonable government support and oversight are essential components of this approach. An atmosphere of cooperation needs to be created amongst stakeholders, and cross-sector bodies, such as UKCCIS, are a great example of this. Funding for research into online behaviours and educational efforts that promote digital literacy and parental engagement, are vital.

19. Effective oversight of industry self-regulatory efforts allows for maximum innovation and development of creative solutions, whilst ensuring that industry continues to raise the bar in the field of online safety. As part of this, FOSI encourages robust and comprehensive industry self-regulation. As a membership organisation, FOSI brings together leading technology companies, who often compete with one another on other issues or for market share, to discuss emerging issues and create best practices and new solutions to increase privacy measures for children and adults alike.

20. There has never been a time when so many resources have been available for parents, grandparents, teachers, and care givers to provide protection from online risks. All of the major operating systems and search engines provide family safety settings and mobile operators, social networks, and Internet Service Providers offer tools and settings to help protect families. Technological parental controls cannot replace involved and empowered parents, but they do continue to be a part of the solution in keeping children as safe as possible online when used to the best of their capacity. Technology develops at a rapid pace, and with each new development companies are working to stay current by creating new and innovative safety tools for parents and teachers.

21. Engaged and knowledgeable parents are vital to ensuring that children have a safe online experience. Providing and encouraging the use of online safety tools is a community-wide effort and each player in the online safety eco-system can play a role in helping parents to learn about and embrace the tools available to them. Parents can be reached through education campaigns through schools or the media, website safety blogs, school initiatives, and government outreach campaigns.

22. Law enforcement must be fully resourced and given the tools and training to combat the rise in cybercrime. Cross-border and cross-industry cooperation is vital to allow law enforcement officials to

⁶⁴ *Ibid.* 7

apprehend and prosecute those involved in illegal online activity, including the creation, sharing and downloading of child abuse material. Similar to the challenges of industry regarding the development of updated parental control software, the ever-evolving nature of criminal activity via the Internet means that providing law enforcement with proper support is essential for the success of their efforts.

23. Superior technology training must be provided to all teachers. This will enable them to incorporate digital citizenship teaching across the curriculum, helping children navigate the online world safely and providing them with the skills to operate in an increasingly technical world.

24. Ideally resilient children would make wise personal choices about the content they access and post online, the people they choose to engage with, and how they conduct themselves overall online. Additionally, as part of the culture of responsibility it is vital to teach children to be media and digital literate.

25. Children must be educated on how to operate as good digital citizens. To know about the rights and responsibilities that come with being online, to understand the consequences of sharing of information and online behaviour and to empower them to make the right decisions when they see upsetting content or inappropriate behaviour. Through teaching children to make good choices on the Internet, they can be better protected from the risks that exist online. The skills that they learn through this process will assist them throughout their digital lives, teaching them to be informed and resilient.

26. The terms of reference of this inquiry examine how best to protect minors from accessing adult content; methods of filtering out extremist material, including images of child abuse and material intended to promote terrorism or other acts of violence; and ways of preventing abusive or threatening comments on social media can all be responded to through the combined use of tools, rules, and educational messaging.

27. It is essential to provide guidance for children on the types of material that they should be accessing, as well as what to do if they come across content that they may find upsetting. Effective promotion of the availability and use of technological parental controls, as well as the need to talk to children about online expectations, will help parents monitor and protect their children from inappropriate content. Finally, regular parental messaging about the importance of good digital citizenship and the responsibilities that associate with being on the Internet will help to ensure that positive experiences are had by all on the Internet.

28. In this submission, FOSI highlighted the research that has been done into online activities and focused on the need to build a culture of responsibility online. Government engagement in the form of funding research, and education efforts for both parents and children forms an important part of the eco-system designed to ensure online safety. Whilst we do not seek to diminish the existence of risks on the Internet, they are no more prevalent than they are in the offline world. While recognising the risks, FOSI wants to ensure that young people can safely access the extraordinary opportunities and benefits of the online world.

September 2013

Written evidence submitted by Terry James

Having been brought up in a Christian household and taught Christian values and principals as set out in the Holy Bible from a child, it is of great concern to me that there is not more protection for young people today from the extremely harmful effects of online pornography.

It is equally distressing to hear of the ongoing abuse of children being used to create pornographic images.

It is the parent's responsibility to protect their children from any type of danger, be it physical or moral, but is also the responsibility of the government to use its powers to take steps to enforce this protection.

If a child by any means has gained access to unsuitable material then that is a sad failure on the part of the parents, the government and the internet providers.

If everybody shoulders their bit of responsibility our children can be protected and must be protected.

As for the ongoing use of the internet for child abuse and pornography, this is an evil that cannot be tolerated. The government has powers it can use to fight this terrible activity. Action must be taken to protect these innocent children from exploitation.

September 2013

Written evidence submitted by the Film Distributors' Association

1. Film Distributors' Association (FDA) is the trade body for UK theatrical film distributors, the companies that release films in cinemas and promote them to audiences, propelling the film value chain into motion. The feature films brought to market by FDA's diverse membership—ranging widely from international blockbusters to classic revivals; and from British films to productions of 42 other countries in 2013—account for 99% of UK cinema admissions. Lord Puttnam of Queensgate CBE is FDA's President. Every theatrical film release is effectively a joint-venture between its distributor and the exhibitors willing to play it, while distributors' launch campaigns typically involve a host of partners, suppliers and media.

2. Theatrical film distribution is a sophisticated, competitive and dynamic business that depends on *product* and the extent to which it connects with *audiences*. With 1% of the global population, the UK generates 7% of global cinema box-office receipts (£1.1 billion from 172.5 million admissions in 2012). The sector operates effectively and delivers a significant contribution to the economy in terms of revenue and jobs, as well as the consequent cultural and creative impacts. An economic multiplier effect applies: for every £1 spent on cinema tickets, at least a further £3 is pumped into the economy on directly related expenditure.

3. FDA welcomes the opportunity to contribute to the inquiry into Online Safety. Film distributors take child protection matters very seriously. Distributors have worked effectively and consistently to safeguard against children accessing inappropriate material throughout the last century. Some film distributors are established, family-trusted brands, known in their own right worldwide, while many others partner on particular projects with brands that appeal to children and young people. For many years, the whole industry has worked in collaboration with the independent British Board of Film Classification (BBFC), in helping to connect audio-visual works with age-appropriate audiences, and better inform those audiences about the content of the works on offer. We know that, in such matters, it is essential to retain public trust.

4. We should like to point out two areas of concern:

- (i) Greater potential for consumer confusion (item 5 below);
- (ii) Dangers inherent in the online piracy of audio-visual titles (item 6 below).

5. (i) Greater potential for consumer confusion:

Film distributors have always worked collaboratively with the BBFC, which celebrated its centenary in 2012. This relationship is relied upon by national and local government, while the published film-specific advice is trusted by the public—for home/mobile viewing as well as cinema visits. Last year's announcement that the BBFC was to be responsible for the classification of content on mobile devices was greatly welcomed as ensuring consistency *across* devices and platforms.

However, this does further underline the potential for public uncertainty where two separate regulatory bodies are responsible for the classification of audio-visual products of significant similarity. Such confusion is most likely to arise when a feature film classified by the BBFC and a video game classified by PEGI are based on the same intellectual property (ie share a source of narrative and characters, such as *The Hobbit*). Inevitably this arises with many of the most popular franchises. Our concern is that parents will naturally make their decisions to purchase/access a video game based on their reliance on the long-established BBFC film classifications, perhaps unaware that the BBFC and PEGI approaches are quite different.

In response to consumer research, the BBFC provides clear and detailed information regarding the content of every film classified in the UK. This is relayed by film distributors and cinema operators on a film by film basis, so that parents may make more informed choices. The more fragmented the regulatory regime across entertainment properties, the greater the scope for user confusion.

6. (ii) Dangers inherent in the online piracy of audio-visual titles:

The film industry has always taken a robust approach to restricting young people's access to inappropriate material—through the BBFC classification system, paid for title by title by film distributors.

As the technological innovations of video and, in turn, DVD placed more responsibility on parents, the industry continued to take seriously its obligation to provide clear information to enable parents to make appropriate decisions for their own children. Today, this is becoming increasingly difficult, as young people *can* access material online in the absence of parental supervision—rendering them vulnerable to what they may find. This problem may be exacerbated by the fact that young people are often more technically proficient than their parents.

FDA supports recent calls by Government and consumer groups for Internet Service Providers to filter (with age restrictions) and appropriately label the content they make available and monetise.

Written evidence submitted by the Information Commissioner's Office

Thank you for giving the Information Commissioner's Office (ICO) the opportunity to submit evidence to your inquiry. Your inquiry is timely, given that the abuse of children via the online services they use is becoming a matter of increasing concern.

We should explain that as the regulator for the Data Protection Act 1998 (the DPA), our statutory interest in this matter lies in the processing of personal data. This takes place where, for example, a company hosts information that identifies someone on its website or where one individual posts information about another on a social networking site. However, as we explain later, our ability to police postings done by private individuals is really very limited.

In our submission we have decided to focus on a limited number of key areas, rather than to explore all the data protection issues that can arise in the context of children's online safety. These are:

1. The DPA's domestic purposes exemption.
2. Privacy notices and explaining personal data issues to children and others.
3. Age verification.
4. What can the ICO do to protect children?

1. THE DPA'S DOMESTIC PURPOSES EXEMPTION

Section 36 of the DPA says that personal data processed by an individual only for the purposes of that individual's personal, family or household affairs (including recreational purposes) are exempt from the data protection principles and other parts of the Act. This means, for example, where one child posts information that is inaccurate (and quite possibly hurtful and malicious) about another as part of a personal online spat, there is nothing action the ICO can take against the child that posted the information—ie we cannot use our normal powers to order the correction of the inaccurate data. However, the organisation that hosts the information cannot itself benefit from the DPA's domestic purposes exemption—we discuss the implications of this later.

The ICO is not calling for a change to the law here. We recognise the importance of the current exemption in terms of individuals' freedom of expression and their need to process personal data for their own reasons without the threat of regulatory intervention. We also recognise the—perhaps insurmountable—logistical challenge of the ICO being expected to police the enormous amount of personal data that private citizens post about each other through social-networking and other means. We doubt if any organisation could take on this task effectively. We also recognise that organisations running services such as social networking sites cannot be expected to check all the information that individuals post about themselves or each other.

It seems to the ICO that the best way to protect individuals who are the victims of abusive postings is for the online service industries—particularly social networking sites and search engines—to be encouraged to develop more effective ways of allowing individuals to have content about them “taken down” or rendered unsearchable. We recognise the practical problems here in that we do not think it is realistic to expect service providers to vet all the content they host, and recent relevant case-law would generally seem to support this approach. (See for example the recent Court of Justice of the European Union: Advocate General's Opinion in Case C-131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González. Note the final judgement here has not yet been handed down.) However, we do think “the industry” should do more to be responsive to the wishes of private individuals to have content about them moderated where it is clearly causing them distress. (This is quite different to public figures being able to hide negative stories about themselves.) However, we are aware of the legal uncertainty and technological difficulty here. We know from our own experience of dealing with determined, well-resourced individuals with access to a great deal of legal and technological resource that, once posted, it may be impossible to remove information from the internet effectively. Content taken down from one site often ends up being posted on another. However, we believe that it is often possible to limit the damage caused by information posted online, if not to eliminate it completely. We urge the industry to do more to develop more effective means of facilitating redress for aggrieved individuals.

We hope that as the information age develops, the legal landscape will become much clearer in terms of the responsibility of online service providers for information that they host, but which private individuals post. We also hope that the technologies that are so impressive in terms of making content searchable and accessible can be used to protect individuals in respect of content that should never have appeared online in the first place. ICO will continue to engage with “the industry” to further these objectives.

ICO has recently published guidance on social networking and online forums—it is available here:

http://www.ico.org.uk/for_organisations/guidance_index/~media/documents/library/Data_Protection/Detailed_specialist_guides/social-networking-and-online-forums-dpa-guidance.ashx

2. PRIVACY NOTICES AND EXPLAINING PERSONAL DATA ISSUES TO CHILDREN AND OTHERS

“Privacy notice” has become the prevalent term in the UK and elsewhere for the information that organisations are required by law to make available to people to tell them, in short, what will happen to any

information they provide to an organisation. This is clearly an important component of online safety for children and others because a properly drafted, accessible privacy notice should allow individuals to make properly-informed information-choices. A privacy notice might allow a child to decide not to provide his or her personal information to a particular website because of the way it intends to use the information.

Privacy notices can only take us so far though, and we suspect that privacy notices largely go unread by adults, let alone children. However, for older, more mentally competent children they do have a part to play—provided they are truthful, accessible, explain the implications of using a service in a particular way and are written in language that the service’s intended users—or their parents or guardians—can understand.

Privacy notices can be particularly useful when combined with relevant privacy-choices. This might be the case where a user cannot navigate through a website unless he or she actively agrees—or declines to agree—to a particular use or disclosure of his or her personal data. However, as we have said, this only takes us so far and it is unrealistic to expect younger children to make meaningful choices here—although obviously parents or guardians could do this for their charges. This is also why it is extremely important that services aimed at—or available to—children are offered with privacy-friendly default settings. This would mean, for example, that service users have to make an active decision to share information about themselves, rather than the sharing taking place unless it is “turned off”. The ICO very much favours a “privacy by default” approach, particularly where children’s data is concerned.

Where services are aimed at children, perhaps more important than the privacy notice is the underlying fairness, safety and transparency of the service being offered—regarding matters such as the disclosure of personal data to third parties, or its use for marketing purposes. We certainly encourage the development of industry best-practice in the area of online services aimed at children, so that there is no confusion—or any unpleasant surprises—when a child uses one of these services. Clearly, marketing that takes place on sites aimed at children should be age-appropriate.

3. AGE VERIFICATION

One approach to the protection of children online is to prohibit certain organisations from offering certain types of service to children below a certain age. (This is the approach proposed in the European Commission’s data protection reform package.) We can see the appeal of the approach in terms of its simplicity—social networking sites should not be allowed to offer their services to children under 13, for example. However, this approach is fraught with practical difficulty and does not tally well with the UK’s legal system which generally relies on a child’s competence, rather than just his or her age, in order to assess whether he or she can make a decision about something. (That said, age-restricted goods are denied to individuals purely on the basis of their age, although we know from “bricks and mortar” contexts how relatively easy it is for individuals under 18 to obtain alcohol, for example.)

However, it is clear that children of the same age have different levels of understanding, and that even quite young children might be able to make informed choices over relatively straightforward propositions. We do think that a too rigid, age-based approach could unfairly restrict children’s take up of on-line services and could deny them the informational learning experiences that will stand them in good stead in later life.

We also recognise the perhaps insurmountable difficulty of introducing a reliable online age verification system—or a robust system for obtaining authentic parental consent. We are concerned that the introduction of such systems could result in service providers collecting large amounts of “hard” personal information about children and their parents—information they would not ordinarily collect.

In terms of age verification, we know that it is usually very easy to register as a user on a site based on a fake identity. A 12 year old can pretend to be 21 and set up a profile on most social networking sites. As a result, children have been able to find their way onto sites that were intended for adults and vice versa.

At first glance, governments, child protection agencies and parents may be pacified by the promise that a single technology will dramatically reduce their child’s risk online and protect them from inappropriate sites and unsavoury characters on the Internet. However, the reality is that age verification is very difficult because a nationally available infrastructure is not available in the UK. If parents and policy architects focus solely on social networking sites, or any single technology solution, then the mark for internet safety will be missed.

There is no quick fix or silver bullet solution to child safety concerns around age verification, especially with the ever changing digital landscape. Tools are available for stakeholders to promote and encourage better, safer online collaboration and communication for children. However, the reliance on a single technology or approach has limitations and possibly is unworkable. We suggest an alternative strategy of a layered approach deployed alongside educational advice, appropriate parental responsibility and supervision, mentoring children in using the Internet safely, ISP involvement, industry protocols, website developers embedding age verification and most importantly using the full range of existing legislation—including data protection law—to protect children effectively. (We have not majored here on the undoubted importance of parental responsibility and supervision. However, we recognise that this is becoming more difficult to provide as we move away rapidly from the shared family PC to the personal portable device.)

The Internet offers countless benefits and learning opportunities for children. It lays the foundation for communication opportunities that have never been experienced by mankind in our history. Because of the

endless benefits it is in society's best interest to help as many children get online. However, we must not focus too much on age verification as a potential silver bullet, but rather focus on a layered approach, allowing children to become ethical, resilient citizens and contributing towards society in a positive manner.

Chapter 2 of the ICO's "Personal Information On-line" code of practice contains more information about the ICO's approach to children's personal data. It is available here:

http://www.ico.org.uk/for_organisations/data_protection/topic_guides/online/personal_information_online

It is worth noting that the European Commission's proposal for a new data protection regulation has several provisions intended to protect children's personal data. In the original text a child was defined as any person below the age of 18 years. However this definition has been removed from the latest draft.

4. WHAT CAN THE ICO DO TO PROTECT CHILDREN?

ICO's activities fall into two basic types—enforcement and education.

We will not go into all the aspects of our enforcement activity here. However, we do have powers that can require organisations processing personal data about children to change their practices in order to comply with the requirements of data protection law. We can also serve a civil monetary penalty of up to £500,000 for a breach. We deal with relatively few enforcement cases relating to children's data—although a growing problem seems to be "scam" text messages being sent to individuals—including children—where the recipient is invited to call a particular premium-rate number in response. Dealing with this type of problem is a major element of our enforcement activity. ICO has been very active here—we submitted evidence and appeared recently before your Committee to discuss the problem of spam messages. Please follow this link for more information about the ICO's work in this area:

<http://www.ico.org.uk/news/blog/2013/more-progress-in-fight-against-cold-calls-and-spam-texts>

We would urge parents, teachers—and of course children themselves—to bring it to our attention when they believe that information about children is being collected, used or shared inappropriately, or where there is evidence that it is not being kept sufficiently secure, for example. We are confident that well-targeted enforcement activity could help to encourage good practice across the board and to marginalise companies that do not handle children's data with sufficient respect.

In terms of the education of children in respect of their information rights, the ICO has been extremely active over the years and plans further activity in the future.

In January 2013 the ICO commissioned a set of education materials covering information rights that were intended to give teachers a creative and engaging set of lesson plans for use in the classroom. The objective has been to raise some key issues with children and young people, so that from a young age they can become aware of their information rights, understand the potential threats to their privacy, and know how to protect themselves on the internet and elsewhere. This is still at an early stage but we are pleased with the initial results.

After pilot lessons at several schools throughout the UK in March and May 2013, nine lesson plan outlines—five for primary schools, four for secondary—have been fully developed and are made available from the ICO's website www.ico.org.uk/schools. Since 18 August 2013, over 3,800 of these education packs have been downloaded. Pre and post lesson evaluation among Key Stage 4 pupils attending High Storrs School in Sheffield showed that awareness of how to protect personal information increased from 59% to 75%, following the lessons.

When appointing the supplier to produce the materials, the ICO insisted that they were designed and developed by teachers still working in schools today and, crucially, were tailored to specific areas of the national curriculum.

The lesson plans explore what is meant by personal data, what information can be shared and which information children should keep safe. The activities help teachers introduce children to their rights and responsibilities relating to data protection and freedom of information, and explain where to go for help if they have a concern. The materials allow teachers flexibility in their approach and encourage active learning, with many opportunities for students to discuss and question.

There are five lesson plans for use in Primary Schools. They are:

Lesson Plan 1—What is personal information?

Learning objective: Children will understand what is meant by "personal information".

LP2—Who needs to know and why?

Learning objective: Children will consider the personal information that it might be appropriate to provide to a given person.

LP3—Opting out

Learning objective: Children will become aware of how to "opt out" from particular uses, sharing etc. of their information. They will understand that information they provide could be used for a variety of purposes.

LP4—How to react to unsolicited messages

Learning objective: Children will consider how they should react to unsolicited emails and text messages that request personal information.

LP5—Rights and Regulations

Learning objective: Children will understand that laws and regulations exist to protect us and to give us the right to access appropriate information.

There are four lesson plans for use in Secondary Schools. They are:

LP1—Strictly Private—what is personal data

Learning objective: By the end of the session, students will be able to:

- explain what they mean by the term “personal data”;
- discuss levels of privacy appropriate to a range of personal data; and
- explain the role of the ICO.

LP2—Private versus public

Learning objective: By the end of the session students will:

- understand how they may unintentionally disclose personal data;
- define the kinds of personal data that should be kept secure;
- list some of the personal data likely to be held about them and the organisations likely to hold it; and
- describe their rights in relation to how organisations should store and use their data.

LP3—Is there something I should know? Exercising our rights

Learning objective: By the end of the session students will:

- understand the main principles applying to how organisations should store and make use of personal data;
- understand that they have choices over how they control their personal information;
- understand how to check that data held is accurate; and
- know how to have inaccurate data corrected.

LP4—No secrets—Freedom of Information

Learning objective: By the end of the session students will:

- understand their right to know under the Freedom of Information Act;
- understand how to make a freedom of information (FOI) request; and
- appreciate the impact some past FOI requests have had on individuals and society.

We are very proud of our achievements thus far in terms of educating children about their information rights and informational safety. We are convinced that the education of children about these issues is crucial in terms of giving them the informational self-defence they will need as children and of course as adults. It is all too easy for children just to provide their details when asked to do so online, or to subscribe to a service because they want the “goodies” without thinking through the privacy implications of their actions. However, we are confident that our educational outreach work will help to foster the critical, questioning attitudes that children’s online safety depends on to such a great extent.

We thank the Committee for the opportunity to provide our views on this extremely important topic. We will of course be happy to provide any further information it requires from us. The point we would like to reiterate is that the issue of children’s safety online is a complex and multi-faceted one. There is no single solution and the best we can do is to make sure that the various organisation—including the ICO—that have a responsibility in this area prioritise the protection of children and co-ordinate their efforts to reduce the risks and enable the benefits of the online world for young people.

September 2013

Written evidence submitted by Virgin Media

DIGITAL MAKES GOOD THINGS HAPPEN

INTRODUCTION

Virgin Media welcomes the continuing parliamentary interest and opportunity to respond to the Committee’s inquiry into the issue of online safety. As a responsible ISP, providing broadband services to more than four million homes and families, Virgin Media puts the issue of internet safety above all others in terms of importance. Debates about these complex issues can often be dominated—on both sides—by a small group of stakeholders with strongly held views. Often the voice of the ordinary consumer has been lost. In this consultation, Virgin Media aims to set online safety in the context of the views of the average UK internet user.

Virgin Media's customers, and the UK public, believe in the internet as a force for economic, societal, educational and personal progress. Overwhelmingly, they believe that digital makes good things happen.⁶⁵

67% agree digital benefits families and enriches life.

Naturally, as consumers they think first about how the internet has empowered them with more product information, comparison and lower prices. But beyond their pockets, our customers tell us they believe in the wider good of digital to strengthen family bonds, contribute to business growth, and enrich their child's education.

They come to that view despite the vast majority of public debate about the impact of the internet on their daily lives focusing on the dangers not the benefits of being online.

76% of media sentiment about the internet is negative.

Of course, those dangers are often very real, serious and demand vigilance from all users if the benefits of the internet are to be enjoyed free from harm.

Our role as a responsible ISP is first and foremost, to encourage that vigilance by educating our customers about where risks do lie, and providing them with the tools to combat those risks how they see fit.

Positively, through education we are seeing that our customers' awareness and vigilance against online risks is becoming increasingly sophisticated. There are understandably knowledge gaps given the subject matter is fast evolving technology, but parents identify a broad range of risks, beyond just the content available online, to include the people their children meet and the personal information that they and their children share.

7% of parents with children under 18 say they wouldn't know how to protect their child online.

As a result, our customers adopt approaches to online safety that best suit the needs and maturity of their families—and they see it as fundamentally their choice as to how they go about that. That often includes applying parental controls, but also involves proactive digital parenting such as putting in place rules around where in the home the internet is used, monitoring usage, and, crucially, having conversations with their children about online safety.

The recent tenor of debate about the online world has failed to reflect the generally positive view that the UK public have about digital and their pro-activity in managing online risks they might encounter. Inevitably, this has led to largely reactive, sometimes knee-jerk policy making in recent months.

Virgin Media is hopeful that moving forward, the parameters and expectations that Government have already set industry in relation to online safety will remain firm and clear, and that future policy is developed in a sober, evidence-based way, taking account of the overwhelming view of the UK public that digital is a force for good.

With that in mind, Virgin Media sees three key challenges for Government:

First to provide certainty to ISPs that an "active choice" approach to parental controls remains the most proportionate, effective way of engaging parents with online safety, and continue to give ISP technical flexibility over the solutions they implement.

Second to focus its efforts on driving engagement amongst parents in these issues through clear advice and education, delivered through evidence-based means that demonstrate behavioural impact.

Third focus Government's resources on tackling child abuse at source through 1. considerably increasing CEOP's resources beyond the 0.08% of Home Office budget it currently has available as it moves into the National Crime Agency; 2. conducting an inquiry into, and developing a strategy to tackle, the wider societal causes of child abuse.

The remainder of this response is divided into three sections:

1. Our customers views about online safety.
2. Our role in delivering a safer internet.
3. A role for Government.

OUR CUSTOMERS VIEWS ABOUT ONLINE SAFETY

Throughout 2012 Virgin Media engaged in a national listening exercise—*Our Digital Future* www.ourdigitalfuture.co.uk—to understand how our customers and British consumers felt about their lives online. Over 3,000 people⁶⁶ were asked about the practicalities of their digital habits—hours spent online, their preferences for content and access—but more deeply, what their reactions were to the growing debate about the balance of risks and responsibilities on the internet.

⁶⁵ Where a specific citation is not referenced, the data is taken from Virgin Media's own consumer research

⁶⁶ The research element of *Our Digital Future* consisted of a quantitative and qualitative survey of 2,000 people conducted by Ipsos Mori; outreach to 1,000 other members of the public through a national listening tour of UK high streets and the *Our Digital Future* website, and in-depth interviews with 15 sectoral experts, MPs and academics.

They were asked about their views on a broad range of online behaviours and risks—access to adult content; sharing of personal data; exposure to malware; piracy—and where they see the balance of responsibilities in protecting children from those risks between themselves, their ISP, and the state.

In summary, we found a UK public that is engaged with the issue of online safety, aware of a range of risks, and confident in taking the actions appropriate for their families to manage those risks in order to make the most of the internet.

BEHAVIOURS AND RISKS

Reflecting the predominant view of the internet's impact on society as overwhelmingly positive, UK parents are generally very comfortable with their children's online behaviour.

17% of parents are concerned about child internet us.

Source: OFCOM Media Literacy Report⁶⁷

Policy makers might conclude that this reflects ignorance or naivety to the realities of online risk amongst parents. However, evidence points to high levels of activism amongst parents, suggesting that their confidence is borne out of a firm view that they have created the right environment for their children to get the most out of the internet.

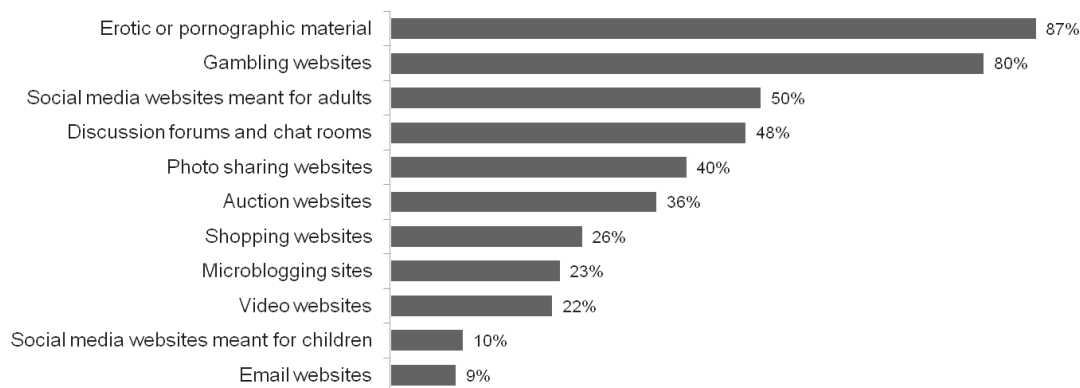
79% of parents have rules in place on internet usage.⁶⁸

84% of parents trust their child to use the internet safely.⁶⁹

7% of parents with children under 18 say they *wouldn't* know how to protect their child online.

In reality, parents have a relatively granular understanding of online risk and can identify a wide range of potentially dangerous channels. As might be expected given the direction of recent public debate, pornography ranks highest as the content that parents are most concerned about their child having access to.

Question: Which sites give you most cause for concern?

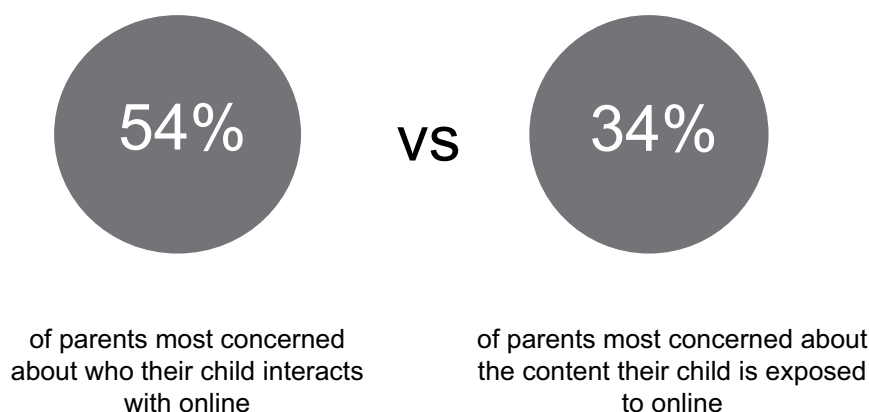


However, access to adult content is only one of a number of concerns for parents. Clearly, there is considerable concern amongst parents about the risks presented to their children through exposure to people they don't know online (so-called stranger danger). In fact, when asked to directly compare risk associated with different types of online activity—as opposed to ranking different types of content—parents registered more concern in relation to stranger danger than exposure to content.

⁶⁷ OFCOM Media Literacy Tracker 2013, <http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/2012-Metrics-Bulletin/2012-Metrics-Bulletin.pdf> page 12

⁶⁸ OFCOM Media Literacy Tracker 2013, <http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/2012-Metrics-Bulletin/2012-Metrics-Bulletin.pdf> page 12

⁶⁹ OFCOM Media Literacy Tracker 2013, <http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/2012-Metrics-Bulletin/2012-Metrics-Bulletin.pdf> page 12



Whilst generally parents have a reasonably sophisticated understanding of online risk, there are gaps in their awareness and understanding.

In part these gaps relate to technological developments that many parents do not fully understand. For instance, whilst in general, parents are well aware of the threats posed by malware and viruses to online safety—70% of customers understand the risks associated with malware—there is limited understanding of how that risk extends to mobile, where only 32% are concerned about the impact of malware.

Other knowledge gaps relate to a lack of exposure to certain types of behaviour. Whilst there is research pointing to high levels of concern about cyber-bullying amongst parents, there was a significant disjunction between levels of exposure to cyber-bullying amongst the parents and children that we surveyed. 47% of children have had some direct experience of cyber-bullying versus 18% of adults with children under 18.

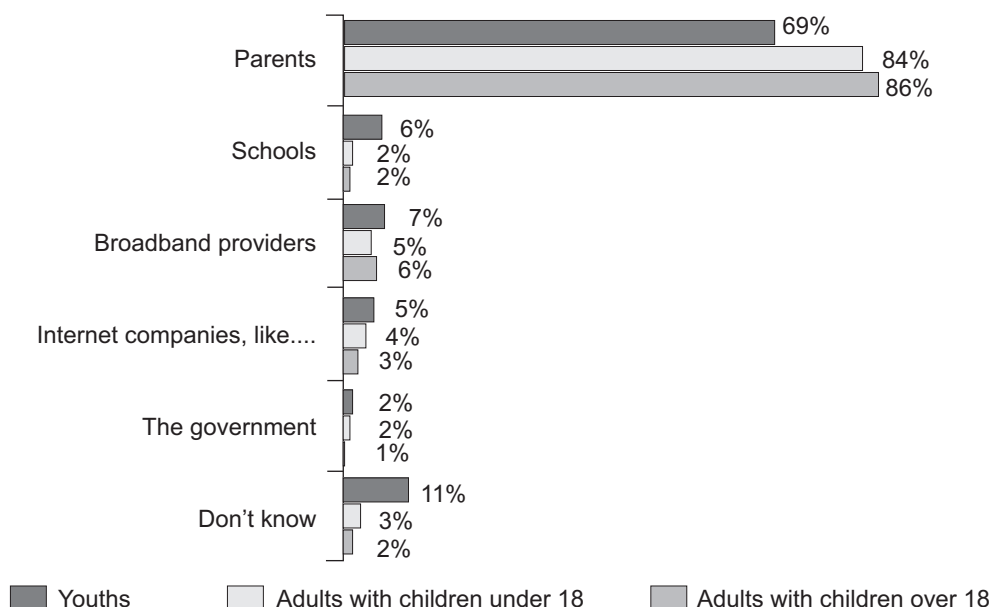
Parents not only identify a variety of risks but in turn adopt a variety of different approaches to digital parenting, reflecting the fact that content filtering—for instance—addresses only one of a range of online risks. A recent comparison of parental mediation strategies across the EU found that the UK has the second highest proportion of parents adopting “All Rounder”⁷⁰ approaches to their child’s internet safety ie, a heterogeneous mix of active monitoring and restrictive technical measures.

RESPONSIBILITIES

In light of the many approaches and activism of UK digital parents, it comes as no surprise that they see themselves as having greatest responsibility for protecting their children online, and are not comfortable with one-size-fits-all approaches imposed by their ISP or the state.

13% of parents comfortable with ISPs setting filtering levels on their behalf

Question: Who has greatest responsibility for ensuring children can use the internet without exposure to inappropriate content?



⁷⁰ http://eprints.lse.ac.uk/52023/1/Helsper_Country_classification_opportunities_2013.pdf Table 3 page 28

That is not to suggest that ISPs, or indeed the state, have no role to play in supporting parents to create a safe environment for their children online. Indeed when asked a slightly different question—who has *some* (rather than *greatest*) responsibility for online safety—parents clearly identify ISPs, schools, central Government and other internet companies as all having a role to play. First and foremost, that role begins with establishing processes in partnership with law enforcement that allow for the removal of illegal content at source. Beyond illegal content, ISPs have the responsibility to use all of their technical expertise to advise parents of the risks and realities of online life, and make available easy to use tools that can support their digital parenting.

OUR ROLE IN DELIVERING A SAFER INTERNET

Virgin Media, as an ISP governed by the EU Telecommunications Framework and E-Commerce Directive, has no regulated responsibility to block consumer access to any content. However we exercise three core responsibilities to help create a safe environment for internet users:

1. Working voluntarily with law enforcement and the Internet Watch Foundation to ensure that child abuse material and terrorism material that they identify is removed from the internet at source, and in the case of child abuse material that is hosted overseas and cannot be removed, is blocked from inadvertent access by our users.
2. Encouraging parents to implement parental controls by providing free, easily installed software and presenting every customer with an active choice.
3. Educating and building awareness of online risk amongst our customers to allow them to adopt holistic approaches to digital parenting.

There is an important and clear distinction between the voluntarily, proactive approach that Virgin Media adopts in collaboration with law enforcement to remove content that they judge to be illegal versus our view on where responsibility lies for accessing legal content. Virgin Media believes that it is for adult internet users to decide whether they or their family can access legal content. Virgin Media is therefore strongly of the view that the industry-led and Government-supported approach to parental controls for legal content, which places the decision in parents hands, reflects the right balance of responsibilities.

CHILD ABUSE, TERRORIST AND VIRUS-CONTAINING MATERIAL

Virgin Media has a zero tolerance policy on the availability of child abuse material (CAM) online, so we take the following steps to help remove it from the internet:

- **Co-founder and top tier funder of the Internet Watch Foundation (IWF).** Virgin Media has supported the organisation's outstanding success in reducing the proportion of CAM hosted in the UK to less than 1% and blocks access to child abuse images hosted abroad.
- **Established a dedicated Online Security Team at Virgin Media** to work with the IWF to process requests, block and remove thousands of pages of CAM from the internet every month.⁷¹
- **Work with CEOP and other law enforcement agencies to support investigation into the production and distribution of CAM.** We support the training of CEOP and other law enforcement professionals through programmes to ensure that they remain up to date with technological developments. We provide in kind support to CEOP by waiving the data costs associated with their work, amounting to approximately £100,000.
- **Implemented splash pages on every blocked url** advising users that the content they are attempting to access is CAM, the legal and personal implications of accessing that content, and signposting perpetrators to the Stop It Now support site.
- **Continued commitment of funding for efforts to prevent child abuse online.** Virgin Media has committed £250,000 over the next four years in addition to our existing funding for child abuse prevention. Part of that commitment will be spent on increased membership fees for the IWF to support expansion of its existing, proactive work. We are in discussions with the IWF and other organisations about how additional funds beyond membership fees might best be used to expand the reach of child protection efforts.

In relation to terrorism content Virgin Media has worked with law enforcement on a voluntary basis to:

- **Establish a process with the Counter Terrorism Internet Referral Unit (CTIRU) for terrorism/extremist content where we host on a Virgin Media homepage.** Under that process, Virgin Media refers suspect content to CTIRU for further investigation. CTIRU review the material and, if judged to be terrorism content, can ask Virgin Media to remove that content, or take no immediate action if that supports their ongoing investigation. That process was established as a trial in 2012 and is now enveloped into the work of Virgin Media's Online Security Team.

⁷¹ The most recent available statistics from the IWF on number of blocked pages is from May 2013 when an average of 189 urls were sent to Virgin Media daily and a total of 3,960 throughout the month.

In relation to content that impacts on the security of our network or our customers' personal data, such as malware, Virgin Media has worked with law enforcement on a voluntary basis to:

- **Establish processes with other relevant law enforcement bodies, such as SOCA, to identify and take action against malware hosted on Virgin Media's network.** Virgin Media also has processes in place to inform customers of malware that may have infected their home device when notified by the relevant law enforcement body. In addition, Virgin Media provides all broadband subscribers with free anti-virus software to help protect their home devices and personal data from malware.

Whether dealing with child abuse, terrorism and virus-containing material, Virgin Media is highly reliant on the expertise and legal footing of law enforcement bodies to make judgements on what action should be taken in response to a particular type of illegal content. Whilst Virgin Media takes proactive steps to minimise the harm of these forms of content, we do not do so unilaterally or without the oversight of law enforcement. In Virgin Media's opinion, efforts to limit exposure to these extreme forms of content are best targeted at removal of the content at source, by the host.

PARENTAL CONTROLS

Virgin Media believes that parental controls can provide one set of tools for parents to help limit harms associated with children accessing adult content online. However, no technological solution is ever infallible, and so it is important that parents see parental controls as just one of a range of things that they must do to create a safe environment for their children online. Virgin Media:

- **Are committed to providing an "active, unavoidable choice" to all new and existing customers** to ensure that each customer decides whether or not they wish to install parental controls. That reflects Virgin Media's view that a "default on" approach to filtering software is not in line with parents expectations that they should make the decision on what content is accessible in their homes.
- **Are introducing a new, free of charge "whole home" parental controls product** to replace our existing device-based client and making that available to our four million broadband subscriber base throughout 2014. Our new DNS based solution is applied at a household router level. It uses the IP address assigned to the subscribers' router to deliver a consistent level of filtering to any and all devices connecting to that home broadband connection. Where a subscriber has opted in to apply the filters, DNS lookups (the URL inputted into the search bar) associated with that subscriber's IP address will be analysed against our block list to determine whether access is permitted.
- **Are making those filters as intuitive and easy to activate as possible, through a simple, "one click" Websafe button** which is pre-selected with the presumption that new customers will want to install filters. We have worked with a range of child safety NGOs and experts to define a list of content categories that will be included in the one click Websafe mode.⁷²
- **Are putting in a place a robust, two-stage age verification process** to ensure that the person making the decision on whether to install filters is the adult account holder. Our closed-loop system will require the account holder to log in using their email address and password before making their "active choice". Following that decision—and any future changes to the level of filtering applied—the account holder will be sent an email with notification of the filtering decision.
- **Are adding layers of sophistication to our parental controls to give parents the flexibility to meet the needs of their households.** Parents have told us that they are not comfortable with one size fits all approaches to filtering that are not adaptable to the digital maturity of their child. So whilst the early version of the product will only offer customers a simple, one-click Websafe mode, as we roll out the product we will also allow parents to select specific categories of content they wish to filter and tailor their filters more uniquely.
- **Are committed to ensuring that child can benefit from a safe internet experience however they access it.** Virgin Media is signatory to the 2003 IMCB Code of Conduct governing mobile internet access, which requires that all mobile operators put in place default filters on adult content across mobile devices. Adult users must request to have the filters removed before being able to access adult content. Additionally, in 2013, Virgin Media worked with UKCCIS to develop a statement on filtering across public WiFi, which commits all providers to apply default filtering of pornography and illegal child abuse material on public WiFi connections, unless the client specifically requests otherwise.

EDUCATION AND AWARENESS

Our responsibility does not stop with providing the tools to block access to content. Nor would that be sufficient to meeting the range of challenges that children face online—covering not just what they see, but

⁷² There are nine categories in our Websafe mode: Child abuse material; pornography; hate; crime; drugs; violence; fraud; hacking; sites that circumvent the filters.

who they meet and what they share. To adequately meet a challenge of this scale, parents first and foremost must be aware of all of the potential risks that their child encounters and need to be engaged in continuing, active, digital parenting. Virgin Media therefore believes that the absolute priority of all online safety stakeholders should be to provide clear advice to parents on the risks their children face online and the steps they can take to ensure their children stay safe. In meeting that priority, Virgin Media:

- **Is a core sponsor of Safer Internet Day and a member of the UKCCIS working group on Education and Awareness.** Working in those partnerships, Virgin Media contributes to efforts to disseminate online safety advice to millions of UK parents. In 2012, over 150,000 people directly participated in Safer Internet Day worldwide and more than 20 million parents were reached with information on child internet safety.
- **Is committed to providing online safety advice directly to our four million customer base through our own channels and materials.**
 - Virgin Media has developed a Protecting Children Matters portal which contains information on all of the child safety tools we make available to customers and practical information on How To Protect Your Family.
 - Virgin Media is currently designing a Child Protection Guide—following on from the *Our Digital Future* big conversation—and app, which will contain new forms of advice and act as a forum for debate and support amongst our parents.
 - Virgin Media has developed a range of video resources on child protection including *Having the Talk*, which introduced viewers to the big issues acting as barriers to greater digital engagement and invited their views.
- **Is committed to using the power of our brand and reach of our marketing efforts to further engage UK broadband users with issues of online safety.** Virgin Media is participating in a cross-industry working group to consider how best to reach customers with these messages and will come forward with detailed plans later in 2013.

A ROLE FOR GOVERNMENT

Virgin Media welcomes the current focus and scrutiny of efforts to deliver a safe internet for children. However, the overwhelmingly negative tenor of recent debate on the subject has not reflected the views of the average UK parent on the digital world, nor the steps that parents, ISPs, Government and other stakeholders are already taking to ensure that children are able to reap all of the benefits that the internet offers in safety. As a result, the direction of policy in this important area has been largely reactive, sometimes knee-jerk, in recent months.

Virgin Media is hopeful that moving forward, the parameters and expectations that Government have already set industry in relation to online safety will remain firm and clear, and that future policy is developed in a sober, evidence-based way, taking account of the overwhelming view of the UK public that digital is a force for good.

With that in mind, Virgin Media sees three key challenges for Government.

First the message from parents is clear—they expect to be in control of setting the rules for their child's life online. "Active choice" is a better vehicle for delivering that than default filtering. **Government should provide certainty to ISPs that an "active choice" approach to parental controls remains the most proportionate, effective way of engaging parents with online safety, and continue to give ISP technical flexibility over the solutions they implement.**

Second filtering is part of the solution to delivering a safe online environment for children but not the whole solution. A robust response to this wide ranging challenge requires vigilant, well informed, and active digital parents. **Government should focus its efforts on driving engagement amongst parents in these issues through clear advice and education, delivered through evidence-based means that demonstrate behavioural impact.**

Third child abuse is a deep rooted societal problem, of which distribution of, and access to, that material online is arguably both a symptom and a driver. The ISP community is therefore committed to ridding the internet of that content—an ongoing, considerable challenge. Virgin Media believes **Government should target its resources on tackling child abuse at source through 1. considerably increasing CEOP's resources beyond the 0.08% of Home Office budget it currently has available as it moves into the National Crime Agency; 2. conducting an inquiry into, and developing a strategy to tackle, the wider societal causes of child abuse.**

Written evidence submitted by the Police Federation of England and Wales

The Police Federation of England and Wales welcomes the review that has been commenced by The Culture, Media and Sports Committee.

1. We believe that the education of individuals and communities to the threats and dangers posed from the on line world is essential in minimising harm and preventing crime. We are of the view that the educational process should commence at an appropriate age and that this should be a continued theme throughout a young person's learning. It is essential that young people understand the vulnerabilities and threats posed to their personal safety, lifelong reputation and wellbeing. We also believe that it is important to encourage responsibility and understanding of the consequence of the misuse of the on line world and rapidly changing technologies.

2. We support a coordinated approach from key public, private and voluntary stakeholders to educate the wider public with the continued risk from those who seek to exploit the misuse of online safety. We believe that a coordinated approach from all partners is vital and that this should be subject of continued review, scrutiny and reporting.

3. We believe that service providers of internet services have a significant responsibility for the on line safety of users.

4. We believe that a joined up approach to internet security should be encouraged and that internet service providers should incorporate full internet security in to their products. A number of companies provide this industry and consumer leading protection package for customers. We believe this could increase security and minimise harm if adopted by all internet service providers.

5. We believe that internet service providers must report to Parliament and the wider community on their actions to minimise the harm from those that seek to misuse on line services. Such an open and transparent mechanism would empower consumers to make an informed decision on whether to use such providers.

6. We support the empowerment of parents, responsible adults and others to prevent and minimise access to inappropriate materials by young persons and others. An industry standard system that blocks access to adult services, explicit pornography and harmful materials should be available all consumers. We believe that this responsibility rests firmly with internet service providers. A failure to develop such a system should in our view require further scrutiny by Parliament and if necessary a legislative framework.

7. We believe that social media providers must provide a timely mechanism for users to report misuse. This will enable those that are being subject to misuse a method to control and stop those who intend to cause harm and distress. We believe it would be helpful for internet service providers to provide support and guidance on their websites for consumers who may require help in dealing with those that misuse on line services.

8. We fully support and encourage closer working relationships between law enforcement agencies, the on line industry and the wider community. These relationships must continue to develop to understand opportunities, weaknesses and threats that may develop with the rapid expansion of technologies.

9. Law enforcement agencies and other stakeholders must be supplied with appropriate resources to minimise the threat from those who would exploit and misuse on line services. It is fair to acknowledge that policing must continually invest in the training and equipping members of staff with the tools to recognise and investigate on line misuse. Without appropriate levels of investment, training and equipping in technologies, the threat of harm and risk will expand. A joined up strategy should be developed by the College of Policing and other key stakeholders to allow the police service and others to maximise resources, understanding and training.

10. It will be important for key stakeholders to recognise threats, weaknesses and opportunities ensuring self-regulation and legislative opportunities are maximised to protect our communities. The sharing of best practice and emerging threats must be a key priority for all, this must be a joined up and coordinated process.

11. A thorough understanding of offending is essential in minimising harm, educating communities and recognising opportunities. The current National Crime Recording Standards in our view fail to record the real number of victims and scale of on line crime. We fully support a review of National Crime Recording Standards to ensure the level of threat is understood, appropriate resources are allocated and threat management is maximised. We are also of the view that there is reluctance from some quarters to report fraud due to possible reputational issues. This is particularly applicable to the finance industry and must be overcome.

12. We believe that criminality has recognised the opportunity to migrate offending to on line services and that offending will continue to exploit such opportunities. The legislative framework to manage offending behaviour that is applied by the criminal justice system should be reviewed to ensure sufficient deterrent and sanctions can be applied.

Written evidence submitted by the End Violence Against Women Coalition

SUMMARY

Online safety is a significant issue for women and girls who are targeted for specific kinds of abuse, harassment and coercion online, just as they are in the offline world. Indeed, there are few spaces online where women are not subject to abuse or discrimination, including social media sites, online pornography and music videos. CEOP's recent report shows that there has been a 70% increase in the proliferation of child abuse images of girls under 10 years old.⁷³

The Home Office leads a cross-government Violence Against Women and Girls Strategy and work on online safety should be explicitly linked to this. Likewise, violence against women and girls should be integrated into policies on media and technology with inter-departmental working on these issues.

There is a clear need for enforcement agencies to be more proactive about tackling online abuse and apply policies and procedures consistently. Likewise, there should be consistent regulation of images across the media, for example consistent treatment of sexualised content in music videos online with videos broadcast on television.

We broadly welcome the approach the Government is taking to tackle pornography, in particular the Prime Minister's announcement that "rape" will be included in the definition of extreme pornography in the Criminal Justice and Immigration Act 2008. This needs to be backed up with public awareness campaigns tackling harmful attitudes and behaviours that are targeted at different sections of the population. Critically, all children and young people have the right to be given the tools to identify abusive behaviour and perpetrator tactics, negotiate online spaces and learn about sexual consent and respectful relationships in school. This should be a legal obligation for all schools to teach in an age appropriate way in both primary and secondary schools. It is also vital that there are specialist sexual violence and other support services for victims/survivors of online abuse, whether or not they report to the police. Such provision is currently extremely patchy, especially for children and young people who are particularly vulnerable to online abuse.

We note that Article 7 of the UN Convention on the Elimination of All Forms of Discrimination against Women states that: "States Parties shall take all appropriate measures to eliminate discrimination against women in the political and public life of the country..." At its Concluding Observations on the UK's compliance with CEDAW, the CEDAW Committee noted that a lack of positive media portrayals of women "contribute to women's disadvantaged position in a number of areas, including in the labour market and in access to decision-making positions, and affect women's choices in their studies and professions."

We are pleased to have the opportunity to respond to this consultation. Our members have considerable expertise on the safety of women and girls and we will focus our response on this group. Our experts are available to give oral evidence to the Inquiry.

1. ABOUT THE END VIOLENCE AGAINST WOMEN COALITION

End Violence Against Women (EVAW) is a UK-wide coalition⁷⁴ of women's organisations, frontline service providers, survivors, human rights organisations, academics and activists who came together in 2005 to campaign for strategic approaches to all forms of violence against women and girls in the UK. We work to the UN definition of violence against women and girls (VAWG) as "violence directed at a woman because she is a woman or acts of violence which are suffered disproportionately by women".⁷⁵

Our members campaigned successfully for the Westminster, London and Wales Violence Against Women and Girls (VAWG) strategies and we run a network of experts on preventing VAWG. Along with several of our members, we gave evidence to the Leveson Inquiry in 2012 about the prejudicial treatment of women in the print media, and we also campaign around VAWG and social media.

2. ABUSE OF WOMEN AND GIRLS ONLINE

Professor Hagemann-White's model of perpetration of violence for the European Commission⁷⁶ identifies the culture of violence in the media and the sexualisation of women and girls as major factors operating at a structural level that contribute to the perpetration of VAWG.

Whilst developments in digital technology over the last decade have made information and support more accessible, they have also massively increased the ways in which women and girls can be abused, threatened and harassed online. There are additional issues for particular groups, such as women and girls with learning disabilities who may be subject to particular abuse and not given the skills to handle it or be able to negotiate issues around safety. Some groups experience stereotyping that intersects race and gender, for example black women and men being stereotyped as "hypersexual" or Asian women as "submissive".

⁷³ http://ceop.police.uk/Documents/ceopdocs/CEOP_TACSEA2013_240613%20FINAL.pdf

⁷⁴ Members include Child and Woman Abuse Studies Unit, Object, Rape Crisis England and Wales, Amnesty UK, Women's Institute, Imkaan, Women's Aid, Eaves, Zero Tolerance, Equality Now, Fawcett, Platform 51, Respect, Refuge, Rights of Women, TUC and others.

⁷⁵ Committee on the Elimination of Discrimination Against Women, General Recommendation No. 19 (11th session, 1992).

⁷⁶ http://ec.europa.eu/justice/funding/daphne3/multi-level_interactive_model/understanding_perpetration_start_uinix.html

The connections with abuse in the “offline” world are also hugely important. Sexually explicit material available in online settings can be used in a range of ways to manipulate and coerce young people into sexually abusive or exploitative activity; for instance, as incitement to perform sexual acts via webcams/Skype which can then be used to blackmail young people into further abuse.⁷⁷

Pornography

- There is now much evidence to show that children increasingly have access to pornography online, whether through smartphones, laptops or other devices, and that this is linked to negative attitudes towards women and relationships, risky and earlier sexual activity. Furthermore, that there is a clear correlation between accessing pornography and violent attitudes. Boys are more likely to deliberately seek out pornography than girls who feel very uncomfortable about their exposure to it (Children’s Commissioner, 2013).⁷⁸

Portman Clinic psychotherapist John Woods has written⁷⁹ about the growing number of young patients referred to the clinic by social services, youth offender services and police for their use of pornography. This includes boys as young as 12 who have convictions for looking at child pornography, as well as children who have committed rape or sexual assaults. This is confirmed by the practice-based experience of frontline service providers such as Rape Crisis Centres who are increasingly dealing with the impact of sexually harmful behaviour in boys at younger and younger ages, often linked to use or exposure to pornography. Rape Crisis Centres also see the impact of the way in which pornography is used as a “grooming” tool by perpetrators of child sexual abuse. It is used as a coercive tool to normalise behaviours in young survivors who are shown pornography to prepare them for what they are told is normal, consensual behaviour.

User-generated pornography and sexually explicit images are also linked to abuse of women and girls. Research on “sexting”⁸⁰ by the NSPCC found that it is linked to abuse, harassment and coercion, and that girls are disproportionately affected.

Social media

On 16 July 2013, EVAW and the Guardian held a round table discussion looking at the relationship between social media and VAWG. Present was Professor Sonia Livingstone who noted how social media has made a significant difference to the way in which we, and young people in particular communicate. Our network of friends is much bigger, and images are far more prominent in communications.

Whilst the problem of abuse of women and girls on social media sites is not a new one, it has recently received a much higher profile in the mainstream media. There are few social media spaces where this is not a problem.

EVAW led the campaigning on **Twitter** against the naming and abuse of the young woman raped by footballer Ched Evans after he was convicted at Caernarfon Crown Court in April 2012. This led to 10 convictions,⁸¹ although many thousands of people were implicated in the abuse. The young woman subsequently had to change her identity because of the abuse that she had received. The issue has made national news once again in the summer of 2013 when feminist campaigner Caroline Criado-Perez and Shadow Crime Prevention Minister Stella Creasy MP received threats of rape and other abuse following the successful campaign to have women on banknotes.

Facebook has also been the focus of concern, prompting a global campaign called #FBrape in 2013 against pages and groups on the site that explicitly promote violence against women and girls with names such as “Why Indian girls get raped” and “Drop kicking sluts in the mouth”. Both Twitter and Facebook host pornography, even though it breaches their terms and conditions. Attention has turned more recently to **Ask.fm** which has been implicated in the suicide of teenager Hannah Smith, after she had been subject to bullying. **Reddit** has a reputation for hosting violent and misogynistic content and CEOP recently warned that live streaming of child abuse through Skype and other platforms is emerging as a growing method of abusers sharing child abuse images.⁸²

Music videos

Robin Thicke’s summer hit “Blurred Lines” has drawn attention to lyrics and music videos that sexualise women and promote violence. The video (banned on YouTube) shows a string of near naked models being ogled by fully-clothed men, with an explicit reference in both lyrics and video to anal rape. Other popular videos by Justin Timberlake and Miley Cyrus also highlight issues around sexist and racist representations of

⁷⁷ See Dombrowski, S C, Gischlar, K L, Durst, T (2007). Safeguarding young people from cyber pornography and cyber sexual predation: a major dilemma of the Internet Child Abuse Review 16 (3) 153–170; Shannon, D (2008). Online Sexual Grooming in Sweden—Online and Offline Sex Offences against Children as Described in Swedish Police Data Journal of Scandinavian Studies in Criminology and Crime Prevention, 9(2), 160–180.

⁷⁸ “Young Men Using Pornography” by Michael Flood in *Everyday Pornographies*, 2011, ed K Boyle

⁷⁹ <http://www.dailymail.co.uk/news/article-2135203/Jamie-13-kissed-girl-But-hes-Sex-Offender-Register-online-porn-warped-mind-.html#ixzz22xJMIlem>

⁸⁰ http://www.nspcc.org.uk/Inform/resourcesforprofessionals/sexualabuse/sexting-research-report_wdf89269.pdf

⁸¹ <http://www.theguardian.com/uk/2012/nov/05/ched-evans-rape-naming-woman>

⁸² http://ceop.police.uk/Documents/ceopdocs/CEOP_TACSEA2013_240613%20FINAL.pdf

women in music. There is increasing understanding of how the sexualisation of popular culture provides a conducive context for violence against women and girls.⁸³

3. SOLUTIONS TO ONLINE ABUSE

Joined up policies

The Home Secretary chairs the Inter-Ministerial Group on Violence Against Women and Girls which has heard from representatives of the music and advertising industry and regulators, and at a separate meeting has discussed new technology. This is very welcome but there needs to be further integration of VAWG in media and technology policies, and vice versa, including regular attendance of DCMS officials at VAWG stakeholder meetings and work with experts in the VAWG sector.

Enforcement and regulation

Recent cases of abuse on social media have highlighted how enforcement bodies may still not be responding adequately to violence and harassment perpetrated towards women online. The Crown Prosecution Service recently published guidelines on prosecutions in cases relating to social media, however it did not explicitly link with its own excellent VAWG Strategy, nor recognise the scale of abuse towards women and girls on social media. Women's groups made submissions to the CPS that gender discrimination should be explicitly recognised in the guidelines and that, in complying with the Human Rights Act, freedom of expression should be balanced with right to respect for private and family life (Article 8 of the Human Rights Act) in conjunction with the prohibition on discrimination (Article 14). Likewise, the police need to take a consistent approach to violence and harassment online and offline for example threats to kill or rape, or stalking perpetrated online.

We believe there is a clear case for consistency in regulation also so that images that would not be broadcast on television or subject to the watershed should also be regulated in media videos, whether offline or online. We note that the British Board of Film Classification has strict guidelines on content in films that promote sexual violence towards women and that its research shows great public concern about such images.⁸⁴ We would like to see regulation across the media take this approach.

We broadly welcome the Government's approach to pornography, as announced by the Prime Minister in July, and in particular we are pleased that "rape" will be included in the definition of extreme pornography. We share concerns with others that filters may block material that is educational, sexual health sites or violence against women support services/campaigns.

Support for survivors

Most victims/survivors of abuse online do not report what has happened to them, as with abuse and violence that is perpetrated offline. It is therefore vital that there are specialist sexual violence and other support services in the community for victims/survivors of online abuse, whether or not they report to the police. Such provision is currently extremely patchy, especially for children and young people who are particularly vulnerable to online abuse.

Corporate responsibility

Much of the focus of recent campaigns about abuse on social media, including Facebook and Twitter, has been directed towards the social media companies themselves. A very important part of the solution is for these companies to have adequate terms and conditions on abuse and harassment in the first place, and for them to be properly and consistently enforced. Whilst YouTube has a policy of not hosting pornographic and sexually explicit content and did not host the Robin Thicke "Blurred Lines" video, it allowed Justin Timberlake's sexually explicit video for "Tunnel Vision" on the grounds that it was "artistic".⁸⁵ Nevertheless, the impact on reinforcing a culture that sexualises and objectifies women providing a conducive context for VAWG was the same. We also believe that music and other creative industries have clear responsibilities not to produce material and images that are discriminatory or harmful.

Education and public campaigns

There is clear evidence from Ofsted⁸⁶ as well as our own research that currently children and young people have patchy access to adequate PSHE/SRE provision in schools and that this is leaving young people vulnerable to abuse and exploitation. As a matter of child protection, all schools should be required to equip young people with the tools they need to understand issues such as sexual consent and respectful relationships, online safety and gender stereotyping. The 2000 SRE guidance is urgently in need of updating to take account of technological developments and to ensure that all forms of VAWG are adequately addressed. This should be

⁸³ Coy, M (2013). Children, Childhood and Sexualised Popular Culture in J Wild (Ed) Exploiting Childhood: How Fast Food, Material Obsession and Porn Culture are Creating New Forms of Child Abuse London: Jessica Kingsley

⁸⁴ [http://www.bbfc.co.uk/about-bbfc/media-centre/bbfc-annual-report-2012](http://www.bbfcc.co.uk/about-bbfc/media-centre/bbfc-annual-report-2012)

⁸⁵ <http://www.rollingstone.com/music/videos/justin-timberlakes-tunnel-vision-ban-lifted-by-youtube-20130708>

⁸⁶ <http://www.ofsted.gov.uk/resources/not-yet-good-enough-personal-social-health-and-economic-education-schools>

backed up by ongoing public campaigns to change harmful attitudes and behaviours targeted at different sections of the community, such as the excellent Home Office ThisisABUSE campaign.

September 2013

Written evidence submitted by Childnet International

SUMMARY

1. Protecting minors from accessing adult material: There are measure that can help here—tools, such as parental controls, ratings and education/awareness of parents/carers and children and young people—but education and awareness underpins all of these.

2. Filtering out extremist material including CAI—the Internet Watch Foundation, one of our partners in the UK Safer Internet Centre are world leaders in this area.

3. Preventing abusive or threatening comments on social media: there are measures that can help here include improving reporting and responsiveness to reporting, and education of children and young people and those who have care of them, and educations underpins all of this.

4. Education is key, and this is an area in need of sustainable support so it can keep pace in this fast-moving environment.

INTRODUCTION

1. Childnet is a registered charity working with children, young people, teachers, parents and carers, government and policy makers to help make the Internet a great and safe place for children. Set up in 1995, Childnet is an independent organisation that seeks to promote the positive use of technology and highlight the positive things that children are doing with new technology, as well as responding to the potential negative side.

2. Childnet's Education Team have for more than ten years worked on a regular basis in both primary and secondary schools across the UK, with children and young people aged from three to 19 conducting targeted comprehensive sessions on e-safety and positive use of ICT technologies as well as considering the risks that school age users may encounter and designing and developing resources to promote safe and responsible use. In the academic year September 2012–July 2013, Childnet staff visited 176 schools, (running on average three sessions in each school), and spoken with 20,800 children and young people aged between three and 18. We also spoke with 2,500 parents and carers and 1400 school staff.

3. Working directly with these audiences is important in helping us to equip them to stay safe online and informs the **resources** that we develop for them. The conversations that we have with them also helps to inform how we develop and respond to **policy** issues and the messages that we take to government and the internet industry about the real experiences of children and young people and what needs to be done to make them safer as well as continuing to provide information and advice to help young people make good decisions whenever and wherever they are using technology.

4. At the heart of all our work is the belief that when used properly the internet is a wonderfully positive tool for children and young people. We strive to take a balanced approach, making sure that we promote the positive opportunities, as well as responding to the risks and equipping children and young people to deal with them.

5. Childnet has produced a range of successful and award winning resources designed to empower the whole school community. In particular, Childnet has previously worked closely with the DoE/DCSF/DfE, BECTA and the TDA on strategic educational projects including the award winning "Know IT All" suite of resources for primary, for secondary, for parents, and for NQTs and Trainee teachers—over two million copies of the KIA for parents CDROM resource were requested and distributed to schools across the UK.

6. In January 2011, Childnet was appointed by the European Commission to be a partner in the UK's Safer Internet Centre, see www.saferinternet.org.uk. In this role we organize Safer Internet Day (SID) for the UK. For SID 2013 we carried out a very large survey of young people—we had responses from over 24,000 children and young people about their online rights and responsibilities and held focus groups with 90 of these young people across the UK to further explore the findings. The right to be educated about staying safe online was voted in the top 10 rights on both the primary and secondary surveys. Evidence from this survey has been included in this response. The full findings are at

www.saferinternet.org.uk/downloads/Safer_Internet_Day/2013/Have_your_Say_survey_-_Full_Report.pdf.

HOW BEST TO PROTECT MINORS FROM ACCESSING ADULT CONTENT

7. The internet is a truly amazing resource which enables children and young people to connect, communicate and be creative in a number of different ways, on a range of devices. The issues and potential risks that minors may encounter on the internet will vary depending on their age and online activities. At Childnet, we have

grouped potential online risks into four categories—conduct, content, contact and commercialism. (www.childnet.com/ufiles/Supporting-Young-People-Online.pdf)

8. There is a risk that when using the internet or other online services and technologies, young people may be exposed to inappropriate content. This may be material that is pornographic, hateful or violent, but it may also be material which encourages activities that are dangerous or illegal, or is just age-inappropriate or biased. In our “Have your Say” survey over a fifth of primary and of secondary aged children said that seeing unpleasant or hurtful things stop them enjoying their time on the internet. The focus group work found that there was a range of types of content that young people find unpleasant online, including scary videos, pictures, chainmail, violent films/games or rude things and swearing.

9. The steps that can be taken to help protect children from this content include **tools**, such as parental controls or filters, **ratings** (such as PEGI for games), **education** (including about the tools and the ratings) and **awareness**. Filters can be a helpful tool in reducing the chances of coming across something upsetting, but is important to recognise that these are not 100% effective and are not to be viewed as a “solution” but rather in terms of being a useful tool. This needs to be clear in any education/awareness work, that this is only one aspect of helping keep children safe online.

10. **The tools:** There are tools available, and these are provided by ISPs, available on Search, on games consoles and other devices. For the successful take up of parental controls there are a number of obstacles to overcome. Firstly, cost, and we see this in the UK overcome by the four big ISPs and the Mobile Operators and others providing filtering for free. Secondly, parents need to know that these tools are available. With Mobile Operators, the tools are default on, so this is perhaps less of an issue, but for ISPs we can see the Active Choice Plus solution which is currently being implemented—once this has been effectively extended to existing rather than just new customers, that will go a great way to making sure that people know about the availability of these tools. Users will have to make an unavoidable choice, “do you want parental controls or not”.

11. **Education and awareness:** However, we believe for this choice to be a meaningful choice it has to be an informed choice. We want to ensure the opportunity provided by the Active Choice is utilized to really help people make a good choice—making sure that parents know what tools are available to them, exactly what it is that they do, how they can be used to best protect their family, and that they are provided for free. At the same time, it should be clear that this is not a solution to keeping your child safe online, and what else you can do.

12. It is a great step that the 4 ISPs are implementing a similar approach to parental controls, ie it is at the wireless router level and covers all devices accessing the home wifi. From an educational and awareness perspective, that uniformity in approach has great advantages.

13. Childnet, in its role as the UK Safer Internet Centre, teamed up with the four ISPs and created a set of “how to” video guides to help parents set up parental controls offered by their internet provider. These videos have been created to empower parents and the ISPs have committed to keeping this video content up to date. These videos can be used by other organizations and can be embedded on other websites, to help get this information out to parents.

14. It is important to remember that filtering and technical tools are only part of the solution in protecting minors online. No filter or parental controls tool is 100% effective, and many of the risks that young people face online are because of their own and other’s behaviour. Parents need to be able to support their children holistically in the online environment as they interact online. At all age groups one of our key messages to children and young people is to “tell” someone they trust—their parents, carers, teachers or school staff if they run into difficulty online. It is therefore important for parents, carers and teachers to talk with children about staying safe online and make sure they know how to respond and what to do if the need arises.

15. We know that this is an area that parents and carers as well as teachers need support in. Face to face outreach work is crucial in this, with children and those that support them, Childnet carries out this face to face outreach work, and the Childnet website (www.childnet.com) contains a wealth of information for children and young people, parents and carers and teachers and professionals. In particular the parents and carers section provides detailed information regarding specific topics such as social networking, online grooming, gaming, as well as conversation starters, a simple and effective way to help parents get involved with their children’s online activities.

16. Schools also have an important role to play in helping to keep children and young people safe online. Childnet responded to the April 2013 consultation on the Reform of the National Curriculum in England stating the importance that “the subject of e-safety is integrated into the formal curriculum both within primary and secondary schools and also within the initial teacher training and school staff continual professional development programmes.” Our partners in the UK Safer Internet Centre, the South West Grid for Learning have been working closely with Ofsted to help bring e-safety standards into schools inspections.

17. Specifically responding to the challenge of protecting minors from adult content online, we believe that schools can help on this topic. The Government guidance on sex and relationships education is now 13 years old, and at Childnet we have joined the Sex Education Forum in calling for the this guidance to be brought up to date, and we see the need to for sex and relationships education to consider technology and safeguarding,

making reference to addressing on-line safety, “sexting” and pornography. Promoting critical thinking about online content including around adult content online, such as pornography, for example, has the potential to develop understanding and resilience amongst young people. We see that schools would need guidance and support to carry this out.

18. There is a need for ongoing educational and awareness work in this area and for this work. As the UK Safer Internet Centre, Childnet (along with the Internet Watch Foundation and South West Grid for Learning) will be running Safer Internet Day 2014 which will take place on 11th February. The theme of Safer Internet Day is “Let’s create a better internet together”. This positive call to action provides all stakeholders with the opportunity to reach out and positively work to empower internet users in the UK.

19. We are hoping a proposed industry-led awareness campaign, led mainly by the 4 big ISPs, can combine with our work and help make Safer Internet Day 2014 even bigger than last SID 2013, which reached 10% of the population, and led to 40% changing their online behaviour as a result of the campaign.

FILTERING OUT EXTREMIST MATERIAL INCLUDING CAI AND MATERIAL INTENDED TO PROMOTE TERRORISM AND/OR OTHER ACTS OF VIOLENCE

20. The Internet Watch Foundation (IWF) is the UK Hotline for reporting Child sexual abuse content hosted anywhere in the world, criminally obscene adult content hosted in the UK and non-photographic child sexual abuse images hosted in the UK. Since 1996, the IWF have worked to reduce the Child Abuse Images hosted in the UK from 18% to less than 1% of the total amount of known content.

21. The IWF is a crucial partner in the UK Safer Internet Centre fulfilling the role of hotline within the Centre. We are proud to work closely with the hotline in the Centre, and to collaborate on joint ventures. For the IWF Awareness Day 2012, the IWF conducted a study which looked into self-generated, sexually explicit images and videos of young people online. The research sought to discover how much of this content was copied from its original source and put on other websites. The findings showed that 88% of the images and videos young people put up appeared on “parasite websites”, meaning they were taken from the original area where they were uploaded and made public on other websites. The study reinforced the message to young people that they may lose control over their images and videos once they are uploaded online.

22. Working in close partnership and in response to this, the UK Safer Internet Centre developed resources providing advice and guidance to help young people consider the consequences of posting sexting images online and what they can do if they find themselves in a position where they have lost control of their images. The preventative resource, “Picture This” is a drama/role play activity designed for use by schools to help young people address the delicate subject matter of sexting. “So you got naked online” is advice on what to do if you have “sexted” and lost control of your images—this resource is designed for young people to be able to use by themselves. The resources can be accessed at: www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals/sexting

PREVENTING ABUSIVE OR THREATENING COMMENTS ON SOCIAL MEDIA

23. As part of the “Have your Say” survey, we asked young people what stops them enjoying their time online. For both primary and secondary age children, people being unkind was one of the main things that stopped them enjoying their time on the internet the most. Almost a third (31%) of primary school age children (7–11s) and a quarter (23%) of secondary school age children (11–19s) said that mean comments or behaviour stops them from enjoying their time online. This isn’t necessarily always what young people would describe as cyberbullying, but can be thoughtless and mean comments and behaviour.

Response to question: What stops you from having fun on the internet?

“People saying my house and movies are rubbish.” (eight year old girl)

“Friends spreading rumours about me and telling other people my account settings or putting some pictures of me on the website that they have changed a little to make it look more silly.” (10 year old girl)

Response to question: What stops you enjoying your time online?

“Seeing screenshots of people saying mean stuff about me, and worrying if people can give my screenshots to other people.” (12 year old girl)

“Video calls from people that you know who used to or still bully you.” (12 year old girl)

“Sick, evil Facebook pages that make me feel sad for the person that’s being targeted.” (13 year old girl)

24. Concern about mean comments is common for both primary and secondary aged children and young people. There is a continual challenge to policy makers and schools to be aware of new services, and their implications. Our research showed that young people do see that they have a role to play in defending themselves and their friends, and it is important to equip them with tools and also knowledge to look after themselves as well as their friends.

25. **Promote digital citizenship:** Education is key. We need to ensure that young people are able to use new technology safely and responsibly whenever and wherever they use the internet. They need to be able to look after themselves, their peers and play a part in the wider community and in essence be good digital citizens. We need young people to learn about what impact their online actions can have on themselves and others, both online and offline, in order to get the most out of the technology. Thinking before you post is a crucial 21st century skill. It is vital that young people are able to learn about this and that parents and carers and schools are able to play their part in this.

26. **Improve reporting:** Industry, or more specifically, the providers of the services used by young people have a clear role to play. In fact there is established good practice for service providers in this area, both at UK level in the UKCCIS advice for industry providers on social networking, moderation, search and chat⁸⁷ and also at EU level in the Safer Social Networking Principles for the EU,⁸⁸ and more recently in the work of the ICT coalition⁸⁹ and the EC's CEO's Coalition to make a better internet for kids.⁹⁰ Included in these good practice self-regulatory documents are requirements or recommendations to have clear prominent and accessible safety advice as well as safety tools for users (such as reporting tools). Many the service providers have signed up to these principles of good practice, and there is the need to ensure that industry are following these principles, as well as ensuring that this expectation is recognised by new services, new arrivals on the scene.

27. Reporting tools are critical in helping deal with abusive and threatening comments on social media. While our Have you Say research revealed that 25% of 11–19 year old social network users say they have reported something online, one in six (15%) social network users age 11–19 did not report because they faced barriers in doing so. Of this number, 43% didn't report because they didn't think it would help (7% of all social network users), 35% because they didn't know what reporting was (5% of all social network users) and 22% because they didn't know how to (3% of all social network users).

28. The reality for children and young people in the UK is that some are still unaware of reporting tools and how to use them. There is a clear need to make sure all young people know they have these tools and are equipped to use them. There is work for service providers as well as educators and parents and carers to make sure that children know and understand what reporting is and how you can make a report.

29. Service providers need to continue to work to make reporting prominent, easy to use and effective. Work needs to be done to ensure young people have confidence in the reporting process and encourage users to make reports and young people need to be reassured about the process of reporting. Facebook have recently launched a "reporting dashboard", where the user reporting can see the status of the report they have made, and can see the outcome of their report, and we see steps like these which create greater transparency and accountability as really important. We would like other service providers to look at taking such steps. Services which do not rely on internal moderation, and rather rely on the reports from their users to moderate the service must do everything they can to make reporting as easy as possible (whilst being effective) and give users confidence in the reporting process.

30. Other bodies can play their part too. For example, the Professionals Online Safety helpline (POSH) run by the South West Grid for Learning as part of the UK Safer Internet Centre provides a great external place where teachers, head teachers and others who work with children can bring their issues/concerns, and the Helpline has developed contacts with the key service providers to be able to escalate these matters and have inappropriate abusive content removed. This is a great and important service which needs more publicity and support.

31. **Conclusion:** Education is key to the issues outlined in this consultation. Whether that be in relation to the tools available, such as the availability and how to use parental controls, or how to find and how to use reporting mechanisms, or to the safe and responsible behaviour of users online. The need is greater than ever with the incredible growth of social media, online content and personal devices, and the access and ownership of technology of children, even very young children. At Childnet we speak to children and young people, parents and carers and school staff, and this face to face work is vital, both in terms of helping to support and inform users or those that care for them, but also to hear from them about the key issues or questions that they have. We develop resources and programmes to help parents and schools support their young people. It is vital to ensure that this work is continued and is supported in a sustainable way going forward, and we would like to see key stakeholders including industry and government playing their part in this.

32. Education is crucial and this work needs financial support to ensure it continues and keeps pace in this fast moving area. We see that there is a clear role for service providers to support education initiatives like that of Childnet and the UK Safer Internet Centre and work in schools empowering young people to engage with and to use social media in a positive way. We have some support from some industry players, but we see that

⁸⁷ <http://media.education.gov.uk/assets/files/industry%20guidance%20%20%20social%20networking.pdf>

⁸⁸ http://ec.europa.eu/digital-agenda/sites/digital-agenda/files/sn_principles.pdf

⁸⁹ <http://www.ictcoalition.eu/>

⁹⁰ <http://ec.europa.eu/digital-agenda/en/self-regulation-better-internet-kids>

education does need more investment and sustainable support in order to ensure its effectiveness in a fast changing environment.

September 2013

Written evidence submitted by Ukie

ABOUT US

The Association for UK Interactive Entertainment (Ukie) is the trade association that represents a wide range of businesses and organisations involved in the games and interactive entertainment industry in the UK.

Ukie exists to make the UK the best place in the world to develop and publish games and interactive entertainment. Ukie's membership includes games publishers, developers and the academic institutions that support the industry. We represent the majority of the UK video games industry; in 2011 Ukie members were responsible for 97% of the games sold as physical products in the UK. Ukie is the only trade body in the UK to represent all the major games console manufacturers (Nintendo, Microsoft and Sony).

We are an Executive Board Member of UKCCIS and sponsored the hugely successful UKCCIS Summit in 2011. The video games industry has taken a leading role in the field of child safety, both online and offline, and continues to do so, as we outline in detail below.

KEY POINTS

- The UK games industry has taken a leading role in protecting minors from adult content, most importantly through the PEGI age-rating system. Ukie led the successful campaign for PEGI's adoption into UK law and constantly promotes safe and sensible gaming to parents, particularly through www.askaboutgames.com
- All the major games consoles have parental controls in place. As well as enforcing the age rating of a game, these controls can be used to limit or prevent children's access to online content through the console.
- PEGI has expanded into the online games world through PEGI Online, setting the same high standard for protection of children from inappropriate conduct. Ukie also work with our members to discuss and share best practice in keeping children safe in online games, particularly through our Online Games sub-group.
- We are concerned about the impact of the government's internet filters plan. There is a potential for this to do significant collateral damage to the UK games industry.

PROTECTING MINORS FROM ADULT CONTENT—OUR TRACK RECORD OF RESPONSIBILITY

The games industry has a long record of taking a responsible approach to child safety, by giving parents the tools to control what games their children play, and how and when they play them. Our most important tool has been the PEGI⁹¹ (Pan-European Games Information) age rating system. PEGI operates through a principles based code of practice, against which content providers across the EU self-declare their practice. A content rating is given by designated national games rating authorities (NICAM and the UK's Video Standards Council), who independently review and monitor self-declaration. The PEGI system itself is also overseen by a number of independent bodies.

PEGI has been in place in the UK on a voluntary industry basis since 2003, when it replaced an earlier UK-only system. It operated alongside BBFC ratings, but having two systems was confusing for consumers. So in July 2012 PEGI became the sole legally-enforceable UK age rating system for games. As a result it is now a punishable offence to sell a game rated 12, 16 or 18 to a child below that age.

All major games consoles incorporate robust parental controls to ensure that these age ratings can be easily enforced in the home. Different manufacturers offer different degrees of control and functionality, but generally they all have the ability to:

- Block the playing of games based on their age rating.
- Block the playback of nonlinear audio-visual content (ie films) based on their rating.
- Disable or restrict access to network functionality including web browsing and messaging.
- Disable voice chat.

These parental controls are password protected and usually offered on an "active choice" basis when the console is first booted up.

⁹¹ The PEGI (Pan-European Game Information) system is a set of ethical standards in the format of a Code which reflect the industry's commitment to act in a responsible manner towards children. The Code's main aim is to provide parents with objective, intelligible and reliable information regarding the minimum age for which a given product is deemed suitable, but the Code also deals with related advertising and promotion, consumer redress & sanctions, commits members not to offend human decency and, after its merge with the PEGI Online Safety Code, now also aims to provide a safe online gaming environment for children.

At the launch of PEGI as the legal UK age-rating system in July 2012, Ukie's members funded a major awareness-raising campaign, under the title Control.Collaborate.Create, educating parents both about the PEGI system, parental controls and about wider issues around children and video games.

Our Control.Collaborate.Create. campaign covered the following key themes:

- **Control**—ensuring that consumers have the knowledge of the tools that they can use to control game content (including PEGI, parental controls and the need to take regular rest breaks).
- **Collaborate**—encouraging parents to engage with and understand the games that their children are playing.
- **Create**—promoting games as a creative, fun and worthwhile activity for everyone.

At the heart of this campaign was the re-launched website www.askaboutgames.com, which is designed primarily to help families understand games. This website prominently features a section linking parents to advice on setting up parental controls for all commonly-available gaming devices, including all major consoles, hand-held devices, and mobile platforms.

The askaboutgames site also plays an integral part in delivering the wider campaign's messages with information and tips for consumers, and showcases of how playing video games is a collaborative and creative experience.

Our campaign had 300 significant media hits, across the BBC, ITV, C4, C5, Sky, national print, games press, regional papers and radio and national online outlets.

Askaboutgames.com has 20,000 visitors a week since its re-launch in July last year. We also distributed more than 50,000 leaflets promoting our safe and sensible gaming messages via Game and HMV stores.

A survey of over a thousand parents was conducted in July 2012 for the start of our campaign to support PEGI. This found that 35.9% of parents who own games consoles use parental controls, either regularly or occasionally, whilst 40% of parents know that parental controls exist for video games but do not use them because they already supervise their children's game-playing and do not allow their children to own or play inappropriate games.

In total, 92.5% of parents whose children played games were aware of the parental controls that existed for those games on the consoles on which they are played.

We do not have previous data on these questions, so we cannot claim to know any trends. However, it is clear that at least three quarters of parents know about the availability of parental controls for games and feel informed enough to have confidence in deciding whether to use them.

This makes intuitive sense—many of today's parents themselves grew up playing games, and have a strong understanding of the medium itself. It also indicates that, although education efforts should of course continue, there is already a strong understanding of the dangers of games both online and offline.

As a result of this strong experience with parental controls and age ratings, Ukie took a leading role in the UKCCIS Parental Controls work-stream and was part of the strong push for an active choice approach, reflecting the good track record such an approach has on games consoles.

PROTECTING CHILDREN IN ONLINE AND MOBILE ENVIRONMENTS

PEGI has been recognised by the UK government as a leading example of an industry taking a responsible approach in keeping children away from unsuitable content, and also has strong recognition amongst UK parents. It has now expanded into the online games market through PEGI Online. As part of the rating process online game providers must indicate if their gaming environments fulfil rigorous PEGI Online requirements which are set out in article 9 of the PEGI Code of Conduct. These are:

- 9.1 **Rated Content:** Products offering Online Gameplay Environments operated by Signatories will, where practicable, be appropriately rated under the PEGI System. This provision will not apply to game content which is posted on the Online Gameplay Environment operated by the User but which is not under the User's control, such as user-generated content.
- 9.2 **Removal of Undesirable Content:** Signatories shall use their best endeavours to ensure that Online Gameplay Environments are kept free of content which is illegal, offensive, racist, degrading, corrupting, threatening, obscene or might permanently impair the development of minors. When Online Gameplay Environments also contain user generated content, Signatories shall use their best endeavours to immediately take down any such content which is illegal, offensive, racist, degrading, corrupting, threatening, obscene or might permanently impair the development of minors. Observance of all the foregoing should, where possible, also include removal of undesirable links or "hyperlinks".
- 9.3 **Appropriate Reporting Mechanisms:** Consistent with the foregoing paragraph, Signatories will ensure that appropriate reporting mechanisms are in place to allow players to notify Signatories of the existence of content such as described in the previous sub-section within any Online Gameplay Environment.

- 9.4 Chatrooms: Signatories should take reasonable precautions to ensure that Online Gameplay Environments which allow voice or video chat, protect children from access to age-inappropriate content introduced by other users.
- 9.5 Other Operators: Signatories shall use their best endeavours to ensure that operators of Online Gameplay Environments offered by Products published by the User and which are authorised by, but not under the control of, the User, abide by these rules and/or subsequently become Signatories themselves.
- 9.6 Safety Warnings: Signatories shall advise users of Online Gameplay Environments under their control of the desirability of taking occasional breaks from Online Gameplay.
- 9.7 Community Standards: Signatories shall ensure the incorporation in their terms of business with users of Online Gameplay Environments of certain provisions usually included under the heading of so called “community standards”. These provisions will contain prohibitions against those users introducing content or indulging in online behaviour which is illegal, offensive, racist, degrading, corrupting, threatening, obscene or might permanently impair the development of minors.
- 9.8 Privacy: Any User engaging in the online collection of personal information from subscribers will maintain an effective and coherent Privacy Policy fully in accordance

Ukie work closely with PEGI to ensure that this system works for games companies, and to continue strengthening and improving it.

Ukie members offer many different types of online game and work to implement tailored safety controls that are appropriate for the different experiences and audiences those games provide. Those may include, among other things, information on safe gameplay, such as taking breaks, or tools to set time limits, chat filters, codes of conduct. See, for example, <https://eu.battle.net/account/parental-controls/index.html>.

Publishers of game worlds aimed at younger children regularly tailor controls to account for that audience’s unique needs. An excellent example is “Moshi Monsters”, the global success created by UK developers Mind Candy.

Children playing Moshi Monsters can post content on pin-boards, which is automatically filtered for inappropriate content. Furthermore, children can only see the pin-boards of the people they invite into their network, which can only be done if the other child’s username is known. This helps to ensure that children are only in contact with people they already know.

These are just examples of the ways in which online game providers are leading the way in allowing children and young adults to interact safely online, while having lots of fun.

Mobile Games—PEGI for APPS and IARC

The rise of smartphones and tablets as gaming platforms has been a vital part of the evolution of the games industry in recent years.

PEGI for APPS, a rating procedure specifically designed for small software applications, including but not limited to games, was launched in 2012 to address this important market shift. It is designed to cater specifically to the needs of app developers and digital platform operators. It is not a new rating system, it is a more flexible and tailor-made procedure that allows mobile or digital platforms to use the classic PEGI rating system as it is known from boxed products and online titles. On top of that, it adds new feature descriptors that inform a consumer about certain types of functionality in an app. Currently, PEGI for Apps is used by Microsoft on Windows 8 and Windows Mobile platforms.

Although app platforms still have local storefronts for customers it has become clear that publishers are in need of a one-stop-shop to get all age classifications for their products in one streamlined process. Therefore, an international working group, including rating boards from Europe, US, Australia, Brazil and others, is working on a global solution under the name of IARC (International Alliance for Rating Content): a list of questions that combines all the criteria of the different rating boards across the globe into one big flowchart.

PEGI for Apps has been part of this project from the start. The IARC program will provide for a streamlined submission process in order to produce classifications for all participating regions at the same time. Although depending on cultural differences, these ratings may vary the system provides a publisher with a single, robust solution and takes away a lot of hassle. IARC is expected to be launched at the end of 2013.

INTERNET FILTERS—SIGNIFICANT RISK OF OVER-BLOCKING

We have particular concerns about the potential for unintended consequences from the universal internet filtering that was announced by the Prime Minister in July.

Ukie have always supported an “active choice” approach to parental internet controls, as emphasised in our response to the DCMS consultation on the issue last year. The approach being proposed, where controls will be switched on by default, goes a step beyond this.

Whilst the protection of children is of course paramount, having controls in place by default greatly increases the importance of ensuring that they are well targeted and do not inadvertently block or restrict access to content that is not in fact inappropriate for children.

We understand that discussions are still taking place with ISPs, and that the final design of the filters is not in place. However, the only example already in place is the filtering that Talk Talk offer to all customers under the HomeSafe brand, and we have specific concerns about this system.

According to the Talk Talk website promoting their HomeSafe technology, parents are given a list of categories of “inappropriate websites” from which they can select which to block. These different categories are:

- Dating.
- Drugs, alcohol and tobacco.
- File sharing sites.
- Gambling.
- Games.
- Pornography.
- Social networking.
- Suicide and self-harm.
- Weapons and violence.

The inclusion of “Games” in such a list is deeply troubling to our industry.

We recognise the value to parents of controls enabling them to restrict access to games that contain mature content (for example when they are PEGI age rated 18) if they choose to do so, as under existing parental controls systems, but simply filtering out all games is an extremely blunt approach that we believe is unnecessary and disproportionate, and could potentially have very adverse effects on the UK games industry. It should be noted that only a small proportion of games are age-rated 18. In 2012, for example, just 9.4% of PEGI-rated games received an 18 rating.⁹² Indeed, in the last ten years just 5.7% of games rated were PEGI 18.⁹³

This proposal seems to ignore the difference between the content and the medium. It would be absurd to have an option for websites about “books” or “films” to be classed as inappropriate by their nature, without regard to the content, nature or rating of the individual products. It is equally wrong for the same to be applied to games.

We strongly disagree with this approach, and are discussing it actively with Talk Talk to learn how it is applied and what impact it is having.

We are very concerned that filtering “games” as a category of inappropriate websites could be held up as an example of best practice: it must not become government policy that this should be adopted by all ISPs. While the industry agrees that the protection of children is tantamount, the solution should be tailored appropriately to address the specific concern and not be so overly broad that it will have extreme and inappropriate consequences.

The potential commercial risk is clear: if a large portion of the UK population had all websites related to games blocked from their internet connection automatically, the impact on the games industry could be significant. More importantly, this filtering would block content that is well outside the scope of the adult material that this program seeks to address.

For example, application of a broad filter for all “games” will create a significant risk that games specifically intended for young people, including educational games, will be automatically blocked by filters targeting those issues.

The game industry does not believe this is in the best interest of UK children or something that parents want or need. This is evidenced in the statistic used earlier in the document that 40% of parents are aware of the parental controls that exist on their games consoles and choose not to use them, as they are already confident that they have sufficient control over their children’s habits. There are a large number of well-informed, technologically savvy parents in the UK, and blocking access to games websites without their consent would do great damage to the system’s credibility.

We strongly recommend that, as the government works with each ISP on implementation of the new filters, it does not promote the inclusion of “games” as a category of inappropriate websites.

Additionally, even filters that more specifically target content about “dating,” “drugs” or “alcohol,” may have unintended consequences that are detrimental to children. For example, a game teaching children about sexual health, drug addiction or other issues is likely to be caught by the filters and so inaccessible to the children it is designed to help. Many of these games can be discovered on sites which are not explicitly labelled

⁹² <http://www.pegi.info/en/index/id/1068/nid/media/pdf/390.pdf> p13

⁹³ Ibid.

as “education” or “charity”, in order to be discovered organically by the young people they are targeted towards, making it even more difficult for filters to intelligently detect and allow them.

Much greater information is needed on how the filters will work in practice, including how quickly incorrect blocks on websites can be reported and removed.

September 2013

Written evidence submitted by The Children’s Society

We are pleased that the Culture, Media and Sport Committee has launched this inquiry into online safety. We welcome the Committee’s focus on protecting children from accessing adult content; filtering out extremist material, including images of child abuse and material intended to promote terrorism or other acts of violence; and preventing abusive or threatening comments on social media. We also support the written evidence submission from the Child Internet Safety Coalition (CHIS) of which we are a member.

We believe that protecting children from accessing adult content can be done most effectively through educating and empowering children to protect themselves online. Whilst filters and blocking software are vitally important, but they will not rid the internet of inappropriate content and behaviour or young people’s access to it. In addition, teachers, parents or carers cannot monitor every single thing their children do online so children need to be taught to make judgements independently and keep themselves safe.

EDUCATING AND EMPOWERING CHILDREN ABOUT INTERNET SAFETY

Only through teaching children about the dangers they may unintentionally expose themselves to online and about predatory individuals seeking to harm them, can we be assured that they will be able to use the internet safely.

The Children’s Society runs nine services that work with children at risk of sexual exploitation and/or have run away from home or care, supporting around a thousand children a year. Our services report that for many of the children we work with that have been groomed for sexual exploitation, this started online in chat rooms, through social media sites such as Facebook, apps or gaming sites. Such sites are a particularly common grooming tool for boys and some practitioners report that approximately 80% of boys are initially groomed in this way, as this example from The Children’s Society in Lancashire illustrates:

Joey (aged 14) met another young man online and they soon became quite close. When they met, Joey realised the man was older than he had initially said but they still began a sexual relationship. Joey believed he was in love and that they were in a loving relationship. Soon he realised he was not the only one and that this man was even older than he had claimed to be. The relationship became violent. We worked with Joey to support him before, during and after the court process and the offender was convicted.

Our practitioners also report that without tailored education and training on the effects of risk taking or displaying overtly sexualised behaviour, as well as the appropriateness of what to post online, young people unintentionally often expose themselves to risks and dangerous individuals who seek to harm and exploit them.

Our practitioners find that sadly most children will be exposed to pornographic images at some stage of their life. Therefore we endorse the Internet Watch Foundation’s statement that “the removal of material alone is not enough, but behaviour change is required through ‘education and awareness’”.

PSHE SHOULD BE A STATUTORY REQUIREMENT AND INCLUDE INTERNET SAFETY

The Office of the Children’s Commissioner (OCC) is also of the opinion that technical measures such as Internet Service Provider blocking and parental measures in isolation are not sufficient and recommended in a recent report that sex and relationships education (SRE) should be compulsory in all schools (“Basically Porn is everywhere”, 2013).

We agree and believe the government should make PSHE a statutory part of the national curriculum and should include internet safety and SRE. We are disappointed that the government has not accepted amendments proposed in the Children and Families Bill to this effect but urge them to accept the amendments at House of Lords stage.

Young people need comprehensive emotional literacy and to learn about sex and healthy relationships alongside digital literacy in order to manage risks online but also to be able to enjoy and use the internet as adults do. Many of our services provide group awareness raising training in schools on how to stay safe online including the signs and risks associated with online grooming, as well as what is appropriate behaviour online.

The government should also do more to ensure that practitioners who work with young people and parents are trained and up-skilled so that they can support and educate young people on online safety.

September 2013

Written evidence submitted by Eric and Esme Bricknell

WE SUPPORT THE CULTURE MEDIA AND SPORT COMMITTEE IN THEIR CONCERN THAT THE INTERNET NEEDS TO BE A MUCH SAFER PLACE FOR YOUNG PEOPLE AND INDEED, FOR EVERY ONE OF US.

My wife and I write as mature citizens and active grandparents who have considerable family responsibilities—towards our children, grandchildren and the wider community. We support the Inquiry which we believe could lead to greater protection, safety and cohesiveness in the family setting.

We believe there are many parents, concerned about what their children can access on the internet, who would love to have some kind of filter to protect them, even from unintentional access to defiling material, but don't have the know-how to install it. By providing such protection by default, the Government will protect these vulnerable households.

We write as having participated in the governorship of an independent school—Focus School, Bramley Campus—responsible for the safety and welfare of successive annual intakes of school children, entrusted to our care by their parents and guardians. These young people are our future—the developing potential who will give character and strength to our country in oncoming years.

We acknowledge the tremendous advantage that young people have in being able to access the internet to tap the stores of information. They can use this positively in their education to produce intelligent responses to questions in any of their subjects. Thus they develop intellectually and academically. We should however protect them during their years of study so that they keep their minds fresh and clear focusing on academic achievement and developing into responsible adults. Nothing will debilitate and detract more than hours of occupation with online programs which arouse lust and can lead to impure relationships.

We write as Christians, treasuring the message of the Holy Bible—the word of God—it provides light to our path and shows what's right and what's wrong. Two very simple, brief examples from scripture: in his letters to Timothy, a younger person, the apostle Paul says “Keep thyself pure” (1 Tim 5v23) and “But youthful lusts flee, and pursue righteousness...” (2 Tim 2v22). These injunctions would powerfully support the expressed concerns of the CM and S Committee.

And then I write as having some years of experience in Health and Safety at my workplace; you identify hazards, eliminate or reduce them and ensure that residual risk is managed for the health and safety and well-being of all concerned. The Government has a DUTY OF CARE, expressed initially in legislation, to eliminate as far as possible the **hazards of moral and physical corruption**, which are to be found on the internet.

So we are very concerned about the danger lurking only a few clicks away from every child—what is regarded as legitimate adult material is defiling and damaging, especially to the minds and morals of young people—and a very large percentage of our young have viewed such material before they have reached the age of 16!

It is most disturbing to see that while the Government has legislated to protect under-age persons from the sale of tobacco products, alcohol, drugs, knives etc, they are left to their own devices when exploring the internet—and less than half of parents have taken the trouble to install filters on their home IT equipment to protect their children!

WE FULLY SUPPORT THIS MOVE BY THE GOVT CULTURE MEDIA AND SPORT COMMITTEE TO INTRODUCE POLICY CHANGES AND TO INVEST IN RESOURCES OF A TECHNICAL NATURE, AND POLICING, TO RESTRICT THE TOO EASY ACCESS TO ADULT MATERIAL.

WE SUPPORT DEFAULT BLOCKING OF ALL ADULT CONTENT AS THE STANDARD SETTING ON ALL INTERNET ENABLED DEVICES SOLD IN THE UK TO STOP CHILDREN SEEING WHAT IS NOT SUITABLE.

WE ASK FOR THE PROVISION OF BETTER AGE-VERIFICATION SOFTWARE

WE SUBMIT THAT WE AS MATURE AGED PEOPLE ARE RESPONSIBLE TO ACT TO PROTECT OUR YOUNGSTERS—DO NOT TAKE THE EASY OPTION OF ALLOWING “FREEDOM OF CHOICE”.

September 2013

Written evidence submitted by Stonewall

INTRODUCTION

1. Stonewall is pleased to respond to the Select Committee's Inquiry into online safety. Stonewall is the leading organisation campaigning and lobbying for lesbian, gay and bisexual equality in Britain.

2. Stonewall's Education for All campaign was established in 2005 to tackle homophobic bullying and create a safe and inclusive learning environment where all young people can focus on their education and fulfil their potential. We work closely with a range of key agencies including the Department for Education and Ofsted, over 60 local authorities and over 140 primary and secondary schools across Britain through the "Education Champions" and "School Champions" programmes to develop strategies for preventing and tackling homophobic bullying.

3. We also work with Government departments, the Crown Prosecution Service and other criminal justice agencies to tackle homophobic hate crime, including abuse perpetrated online. We support media and technology providers to respond to homophobic abuse posted on their websites and to share best practice.

SUMMARY

4. Stonewall supports efforts to make sure that young people are protected from inappropriate material on the internet. Many gay young people don't have access to information about lesbian, gay and bisexual issues elsewhere and rely on the internet for support. This can lead to them accessing inappropriate content such as adult dating websites and porn sites.

5. Internet filters to protect minors from adult content mustn't however block content that is helpful for gay young people. It's important that young people are able to access age-appropriate information and support on the internet about lesbian, gay and bisexual issues, as well as peer support. Gay young people should also be able to access information and advice from their school and local authority.

6. Stonewall is concerned about the high prevalence of homophobic abuse posted on the internet. This can have a profound impact on gay young people as well as gay adults, leading to feelings of vulnerability as well as more severe mental health problems. Stonewall wishes to see criminal hate speech committed online effectively prosecuted. We also wish to see robust measures carried out by media websites and other technology providers to respond to and prevent homophobic content being posted on their sites.

PROTECTING MINORS FROM ACCESSING ADULT CONTENT

7. *The School Report* survey of over 1,600 gay young people, conducted by the University of Cambridge for Stonewall, found that more than half of gay young people are never taught anything about lesbian, gay and bisexual issues at school and 85% of gay young people are never taught in school about biological or physical aspects of same-sex relationships. More than half of gay young people don't feel there is an adult at school who they can talk to about being gay, and one in four don't have an adult to talk to at school, home or elsewhere.

8. In many cases this will be because they don't feel ready to disclose their sexual orientation, or worry about a negative reaction from doing so. However, even those young people who are open about their sexual orientation often struggle to get the advice that they need because parents and teachers lack an understanding of the issues affecting gay young people.

9. As a result, one in ten gay people aged under 18 use dating websites for gay adults to meet other gay people and learn about gay life, despite the significant risks this poses for young people. Many seek information from porn sites, which is likely to be inappropriate and inaccurate.

10. We believe access should be restricted to adult dating sites, as well as to adult dating apps, to make sure gay young people are protected from sites where they may be vulnerable to predatory behaviour or that may expose them to images unsuitable for children and young people. Restricting access to features such as webcams and cameras on phones and computers would also help protect young people from being exploited.

11. The internet is however an important source of information for gay young people who may be experiencing issues relating to their sexual orientation, including the 55% of British school pupils who experience homophobic bullying. There are also some educational sites that provide accurate information and advice about the biological and physical aspects of same-sex relationships, including about safer sex and STIs, which should be accessible to make sure young people can access information that keeps them safe.

12. The internet also connects gay young people with other young people who may be experiencing similar issues and feelings and who can offer peer support and friendship. *The School Report* found that, although over half of gay young people would like to go to a specific youth group for gay people, 72% do not have access to such a group or are not aware whether one exists in their area. As a consequence almost two thirds of gay young people use the internet to meet other lesbian, gay or bisexual people. Two in five lesbian, gay and bisexual young people use social media, such as Facebook, and more than one in three use websites for young people, such as dedicated online youth forums.

13. Stonewall is concerned that, from our experience of working with schools and local authorities which use filters, they very often block key words that relate to gay people such as “gay” and “sexuality”. *The School Report* found that one in three gay pupils say they can’t use school computers to access resources or information online about gay issues and a further 36% don’t know if they can. One respondent to the research reported pages about Oscar Wilde being blocked by a school’s internet service provider due to words relating to his sexuality.

14. It is important, therefore, that adult internet filters only restrict content which is harmful or inappropriate to young people. Filters should not block access to age-appropriate information and support, including peer support, for gay young people and those who experience homophobic bullying.

15. It’s also important that schools provide gay young people with information and support about lesbian, gay and bisexual issues so that they are not overly reliant on the internet as their only source of information. Schools should integrate sexual orientation issues across their teaching and should ensure that they stock books and resources that talk about gay issues and that reflect different families, and provide a list of safe websites that provide support and information for gay young people.

16. Local authorities also have a statutory duty to ensure young people have access to sufficient leisure-time activities, which are for the improvement of their wellbeing and personal and social development, and to ensure that such activities are publicised. Local authorities should have advice and support pages and information about services for gay young people available on their youth service’s website and staff should be aware of these so they can promote them to the schools and youth services they work with.

PREVENTING ABUSIVE OR THREATENING COMMENTS ON SOCIAL MEDIA

17. Stonewall has additional concerns about the deeply offensive homophobic language and abuse frequently posted online. *The School Report* found that almost one in four lesbian, gay and bisexual pupils experience cyberbullying on online message boards, blogs and social media sites such as Facebook. Forthcoming Stonewall research will reveal the extent of homophobic abuse experienced by lesbian, gay and bisexual adults online.

18. This high prevalence of homophobic insults is reflected on the website www.nohomophobes.com, which measures the usage of homophobic language on Twitter. This website has found that on average the word “faggot” is used on Twitter over 45,000 times daily and “dyke” is used over 4,000 times daily.

19. Stonewall believes the prevalence of such language online contributes to a climate in which lesbian, gay and bisexual people feel insecure and vulnerable. Homophobic comments have many victims since they target not only individuals but lesbian, gay and bisexual people in general—with the number of potential victims increasing with the size of the audience. Comments posted by high profile figures such as professional sports personalities are likely to be seen by many followers, including young followers, and corroborate the negative messages about gay people experienced elsewhere.

20. The consequences of this abuse can be severe. Lesbian, gay and bisexual young people who are bullied are at higher risk of suicide, self-harm and depression, with almost a quarter saying they have tried to take their own life. *Homophobic Hate Crime: The Gay British Crime Survey 2008*, based on YouGov polling commissioned by Stonewall of over 1,700 lesbian, gay and bisexual adults, found that homophobic hate crime has a significant impact on gay people’s feelings of vulnerability, with one in ten saying that being a victim of crime is their biggest worry. Stonewall is concerned that the ease with which people can post homophobic abuse online makes them far more likely to do so, particularly where they can do so anonymously.

21. For these reasons Stonewall welcomes the publication earlier this year of Crown Prosecution Service guidance on prosecuting cases involving social media. We believe that, while many homophobic communications posted online will not meet the threshold of criminal hate speech, the criminal justice system must respond to those communications that would warrant prosecution if committed “offline”. This includes language and behaviour that incites hatred of or violence towards gay people.

22. Stonewall also wishes to see media organisations and technology providers effectively moderate offensive content posted on their websites. Many already have policies in place for moderating offensive content that are more stringent than the law, which we welcome. In addition we wish to see better sharing of good practice between providers, as well as measures to restrict users from posting content anonymously. We also wish to see clear guidance made available to individuals on how to report online homophobic abuse and why it’s important for them to do so.

23. We believe it would be helpful for the Crown Prosecution Service and other criminal justice agencies, as well as relevant Government departments, to work collaboratively with service providers to encourage and support them to prevent homophobic abuse being published on their websites.

Written evidence submitted by FPA and Brook

ABOUT FPA

FPA is one of the UK's leading sexual health charities. Our mission is to help establish a society in which everyone has positive, informed and non-judgmental attitudes to sex and relationships; where everyone can make informed choices about sex and reproduction so that they can enjoy sexual health free from prejudice or harm.

We do this through providing a comprehensive sexual health information service for professionals and the public, running community based sex and relationships education programmes and campaigning to ensure that high quality sexual health information and services are available to all who need them.

To find out more about FPA and the work we do please visit our website: www.fpa.org.uk

ABOUT BROOK

Brook is the UK's leading provider of sexual health services and advice for young people under 25. Our mission is to ensure young people can enjoy their sexuality without harm. Brook services provide free and confidential sexual health information, contraception, pregnancy testing, advice and counselling, testing and treatment for sexually transmitted infections and outreach and education work, reaching over 290,000 young people every year.

Brook believes that every young person in Britain deserves sex and relationships education (SRE) that is relevant to them, focuses on relationships as well as sex, honest about human sexuality and taught by professionals who are well prepared and confident. Sex and relationships are a life skill, as important to our future health and happiness as any other subject, and young people deserve to be heard.

To find out more about Brook visit: www.brook.org.uk.

SUMMARY

Brook and FPA welcome the focus on protecting young people from harm. Young people are vulnerable from online environments in a number of ways, which are not just about access to pornography. These include grooming, bullying and exploitation, and it is important that this Inquiry does not seek to disproportionately focus on pornography in comparison to these other important areas of consideration. Certainly, we know that simply blocking internet content is not a cure-all, and the role of education in supporting young people's safe navigation of the online environment is key. Therefore we strongly advise for the need to talk about education for young people and support for parents at the same time.

In particular, we would be concerned if actions resulting from a review of filtering meant that legitimate education websites were blocked as well.

In summary:

- We welcome the focus on protecting young people from harm, however we know that blocking pornography at the source is not a cure all, and the role of education is key.
- We would be concerned if the block meant that legitimate education websites were blocked as well.
- Finding a way to protect and educate young people will require a solution that involves everyone—digital companies, government, parents, schools, communities and, crucially, young people themselves.
- In particular, we are concerned about the absence of young people's voices in this debate, and this response encompasses views from young people from across Brook's national range of services. We would welcome further dialogue with young people from this Inquiry, which if required, Brook and FPA would be happy to help facilitate.
- The Government should better support parents to help their children in navigating technology with which they are not familiar.
- Sex and Relationships Education (SRE) guidance pre-dates recent and emerging issues on technology and safeguarding, with no reference to addressing on-line safety, "sexting" or pornography in SRE. Brook and FPA recommend that the Government should update SRE guidance for the modern era.
- We recommend enacting a help/whistleblowing button on websites so that children can be immediately directed to reputable professional organisations and get advice about what they have seen.
- The Government should implement policy which leads to pornography websites showing the consent and negotiation that leads to the sexual acts which are shown.

BROOK'S YOUNG PEOPLE'S RESPONSE TO THIS INQUIRY

To inform this response, Brook asked groups of young people across the country to consider their views of the questions and themes raised in this Inquiry.

These groups included young people who identified as LGB and T (Lesbian, Gay Bisexual and Transgender), male, female and non-binary, BME (Black, Minority, Ethnic communities), experience of mental health, experience of homelessness, and as young offenders. A summary of their conclusions is provided here and a full copy of the report can be found in Annex A of this document.

CONCLUSIONS FROM YOUNG PEOPLE'S RESPONSE

"If young people want to access porn, out of arousal or curiosity, that's perfectly healthy and typical. However, easy access to porn needs to be supplemented with good sex education and lessons about internet awareness and safety, as well as an open and non-judgemental societal attitude towards sex and sexuality."

(anonymised quote from young people's response)

The feedback from the young people shows that, broadly speaking, it is clear that young people need better, more inclusive education on internet safety, both for children and for parents, not least to ensure that knowledge, skills and understanding around online safety are embedded in the next generation. This would support a societal shift in the bullying culture which has developed around social media, without imposing enforced censorship which could inhibit young people's ability to access accurate information about sex.

Compulsory education on internet safety, covering issues which include pornography and cyber bullying, would allow young people to explore and understand their developing sexuality whilst reducing any risk of harm.

RESPONSE TO QUESTIONS

1. How best to protect minors from accessing adult content?

1.1 In order to protect minors from accessing adult content we must provide young people with the support, education, skills and understanding to ensure that they are not damaged by, pressured into or exploited through exposure to porn and that they are able to cope with the availability of pornography, on and offline.

1.2 However, Brook and FPA do not believe that it is possible or right to simply prevent young people accessing pornography. We make a clear distinction between child abuse and pornography, and indeed censorship and protection. We also welcome the focus of this Inquiry on protecting young people from harm and condemn all images of child abuse, which are illegal.

1.3 Brook's research with groups of young people suggests:

- While many young people have concerns about pornography and would like help and support dealing with it, we must talk about education for young people and support for parents at the same time.
- From a sample of young people that we spoke to 28.6% said they have used porn to try to find out more about sex, which is typical of the conversations we have had with young people on this topic. We also know that young people would prefer to find out information on sex from other, more reliable sources (like school, or their parents) but that this is not always available to them.
- Although the majority of young people did not think that porn was like real sex; many are concerned that it creates unrealistic views about relationships.
- One indicative quote from this group said: *"instead of stopping young people watching porn... the focus of the debate should be around teaching young people the differences between porn and reality"*.
- Only 2.1% of the sample group of young people we asked had never seen any porn.
- 58% of young people in our group had seen porn online by accident when they were looking for something else. This has an implication for how search engines help to filter "educational" vs "porn" materials through common search terms young people may use.

1.4 In terms of how young people would like to better deal with pornography they may see, Brook and FPA recommend an educational approach which helps young people to:

- Understand the context of porn—ie it is not real life.
- Respond to pressures in relationships as a result of it.
- Find the information currently found in porn from someone/somewhere reliable.
- Know how to resist pressure to watch.
- Know what to do if they see it by accident.

Parents

1.5 Brook and FPA believe that parents should be better enabled and encouraged to take responsibility for supervising their children and setting appropriate safety settings, particularly if they have young children who may be vulnerable to seeing images that they might find distressing. The young people we spoke with pointed out that there are existing safety settings which are very good filters. They felt that if safety settings are used appropriately then young people would not come across adult content when searching for something else.

"We don't need to create new filters, we just need to educate parents about how to use existing safety settings." Young woman, 16.

"Educate the parents, who can in turn educate the children." Young person, 18.

1.6 To enable parents to act accordingly, they suggested that education should be provided to parents so that they are able to understand and set parental controls. The young people that Brook spoke to all knew how to set controls themselves, describing the process as simple, and felt that with the right level of intervention and education from parents, there should be no reason why children should see adult content if they or their parents deem the material disturbing. They suggested developing leaflets, posters or training/workshops for parents, explaining how simple it is to set these controls.

"Educate parents on how young people access what they do and make it so that young people know that they can talk to their parents or someone they trust if they have seen something that makes them distressed." Young person, 20

"Individual guidance by parents to ensure children don't find this material. If a parent is present, even if they do find it, it can be explained properly, explained why it's wrong and why not to go back to the site." Young person, 18.

1.7 Parenting support programmes such as the FPA's Speakeasy⁹⁴ programme (see below) can help parents build up the knowledge and skills they need to enable them to discuss issues around sex, relationships and growing up with their children and teach them key skills in these areas. In turn, developing a stronger dialogue between parents and children can help build the confidence of the children to be more open with their parents about what they may have seen.

Speakeasy

1.8 Speakeasy⁹⁵ is a FPA course for parents and carers to better enable them to engage with the children for which they are responsible, on often tricky issues surrounding sex and relationships. FPA knows that many parents and carers want to talk with their children about issues associated with growing up, including sex and relationships, but many are embarrassed or unsure about where to start and what to say.

1.9 FPA has developed the Speakeasy programme to enable parents and carers to develop the skills, knowledge and confidence to have these sometimes difficult conversations. The community-based project runs over eight weeks and covers factual information including how to keep children and young people safe; the pressures young people may be under; and strategies for proactively starting discussions on growing up, sex and relationships. The course is accredited by the Open College Network, which gives parents the opportunity to receive credits for the work they do, which they can then apply in further learning or in employment.

1.10 Evaluations of the project have demonstrated the positive impact it has on parents' knowledge, confidence and their relationships with their children. A Social Return on Investment (SROI) analysis of the programme has estimated the total value of benefits to children and parents and to the state to be £21 million. The value to the state represents a return of £5.29 for every pound of public money invested in the project.

Sex and Relationships Education (SRE) and the role of schools

1.11 Brook and FPA believe that parents and carers play a crucial role in giving information and advice to children and young people about sex, relationships and growing up. However, although parents and carers absolutely have a role to play in protecting minors from accessing potentially damaging online material, according to the National Association of Head Teachers, 83% of parents also had sufficient confidence in schools' ability to help their children understand the dangers specifically associated with pornography, and that they believed teachers were as important as parents in handling the issue. Just 13% thought it should be left to parents alone to educate children about pornography (NAHT survey, May 2013).⁹⁶

1.12 Indeed, Brook and FPA strongly believe SRE must cover many issues relating to this Inquiry beyond porn, including sexting, making friends and relationships online, bullying, and safety in relationships.

1.13 In order to achieve this, Brook and FPA believe that the best strategy is a joint home-school programme between schools, parents and young people. We should also acknowledge that many parents, despite their best intentions, will still feel too awkward to have conversations about sex with their children. Furthermore, schools are widely regarded as an appropriate and impartial ground for such discussions.

⁹⁴ Further information on Speakeasy: <http://www.fpa.org.uk/communityprojects/parentsandcarers>

⁹⁵ Further information on Speakeasy: <http://www.fpa.org.uk/communityprojects/parentsandcarers>

⁹⁶ NAHT survey, May 2013

1.14 This sentiment is supported by Brook's discussion with young people who said that internet safety should be taught in school, including about how to set controls. Brook and FPA support the young people's suggestion that educators could explain to children that there are images on the internet which may not be suitable, talk to them about what it means, and teach them how to avoid it. Furthermore, children should be taught that there are some things on the internet that they may find disturbing and that there are people they can talk to if they do see something that upsets them.

"I think education is more important than sheltering young people and just pretending they are not there, because they would no doubt find them anyway." Young Person, 18.

"Better education in schools. Explain to them that those films are not real, and are actors." Young person, 20.

"I think educating young people on the different types of images etc is also important to ensure that when they are faced with such things they know how to deal with them." Young person, 23.

SRE and the prevention of sexual abuse, sexual exploitation and domestic and sexual violence

1.15 In its May 2013 report into PSHE, Ofsted states that lack of age-appropriate sex and relationships education may leave young people vulnerable to inappropriate sexual behaviours and sexual exploitation, particularly if they are not taught the appropriate language, or have not developed the confidence to describe unwanted behaviours, or do not know who to go to for help.⁹⁷

1.16 SRE can play a role in keeping children and young people safe. SRE aims to equip children and young people with language and skills to understand appropriate and inappropriate behaviour, be able to resist pressure and to know who to talk to and how to access help and support when they need it.

1.17 Specifically Brook and FPA believe that in the context of online safety, SRE could be used to teach young people as follows:

- To manage situations where they are feeling pressured into sex, or to act in a sexual way.
- To address sexual consent and sexual coercion.
- What is acceptable and unacceptable in terms of sexual advances.
- What is not only acceptable and unacceptable, but also legal and illegal in terms of "sexting" (the act of sending sexually explicit messages and/or photographs).
- To be respectful, particularly in the context of widespread availability of pornography, which raises unrealistic expectations.
- How unacceptable it is to engage in violence or abuse against women who refuse sex.

1.18 The backing for this is clear. In May 2013, a YouGov opinion poll found that 86% of UK adults believe that sex and relationships education "which addresses sexual consent and respectful relationships" should be compulsory in secondary schools.⁹⁸

Fantasy vs Reality course⁹⁹ and training resource¹⁰⁰

1.18 FPA has developed a course and booklet which supports teachers to deliver a series of lessons exploring the influence and impact of the media, the internet and pornography on the sexual attitudes and behaviour of young people.

1.19 These resources help teachers to plan lessons on the very sensitive subject of the sexualisation of young people, including the role of pornography. It also provides objective, safe and creative ways to tackle the issue.

1.20 These resources meet official guidance for students at Key stages 3 and 4 with, and include different lesson plans and training options for each stage. The booklet also includes a CD-ROM with video clips, images and PowerPoint presentations suitable for use with Key stage 3 and 4 students, and was produced by the Brighton & Hove Healthy Schools Team and developed in partnership with PSHE (Personal, Social, Health and Economic) education teachers with guidance from the Metropolitan police and FPA staff.

Relationships, Safety and Risks booklet¹⁰¹

1.21 Brook has developed a booklet, which offers insight, signposting and support around the everyday risks young people face as they navigate the worlds of social media, the internet and their own social lives; at home, in education, and when out and about.

⁹⁷ Not yet good enough: personal, social, health and economic education in schools, Ofsted, May 2013

⁹⁸ YouGov Opinion poll commissioned by the End Violence Against Women and Girls Coalition, May 2013

⁹⁹ Further information about FPA's Fantasy vs Reality course can be found here: <http://www.fpa.org.uk/course/fantasy-vs-reality-impact-and-influence-pornography-young-people-0>

¹⁰⁰ Further information about FPA's Fantasy vs Reality training resource can be found here: <http://www.fpa.org.uk/product/fantasy-vs-reality#product-content>

¹⁰¹ Further information about Brook's Relationships, Safety and Risks Booklet can be found here: <http://www.brook.org.uk/index.php/resources/resource-types/ask-brook-booklets/ask-brook-about-relationships-safety-and-risks-detail>

1.22 The booklet gives an overview of a wide range of potential issues; including “sexting”, sexual bullying, pornography and unhealthy relationships. Crucially, it offers relevant information and tips for staying safe as well as details of where young people can go if they need help, support and advice.

1.23 *Ask Brook about relationships, safety and risks* is a brand new addition to the pocket-sized A6 Ask Brook booklet range. It is aimed at 14+ young people and an extremely useful tool to all professionals working with youth groups and young people.

Updating current Government guidance re SRE

1.24 Currently, maintained schools must have regard to the (as was) Department for Education and Employment’s, *Sex and Relationship Education Guidance* (2000). This guidance pre-dates the Sexual Offences Act 2003, the repeal of Section 28 of the Local Government Act and the 2010 Equalities legislation which includes the recommendation that schools teach gender equality and non-violent, respectful relationships between women and men. This current Government SRE guidance also pre-dates recent and emerging issues on technology and safeguarding, with no reference to addressing on-line safety, “sexting” or pornography in SRE.

1.25 Brook and FPA recommend that the Government should update SRE guidance for the modern era.

2. How best to filter out extremist material, including images of child abuse and material intended to promote terrorism or other acts of violence?

“When children start to hit puberty, then without places where they can talk about sex in a positive way (and not just mechanics) then they will go looking for potentially harmful images, and in the world we live in it is virtually impossible to censor those completely.” Young person, 18.

2.1 Any proposal to restrict young people’s access to extreme material online will be fraught with complication and difficult to implement. Filters must be sophisticated to allow for a range of factors (for example, households with children of different ages, and differing definitions of pornography). Part of supporting young people through education is ensuring they have access to good quality, factual information on sexual health online. Attempts to restrict young people’s access to pornography may inadvertently lead to the blocking of good quality education sites.

2.2 Although young people have told us that while they are concerned about pornography and would like help and support dealing with it, we must also acknowledge that a block can only go so far and as discussed in our response to Question 1, we should ensure we promote the need for education for young people and support for parents at the same time.

Defining “extremist”

2.3 Brook and FPA support the views of the young people interviewed by Brook and that it is important to give consideration to what is deemed “extremist”. They were clear that images of child abuse or bestiality should be banned, but some felt that censoring images of bondage, for example, is wrong because acts of bondage may be consensual. They were clear that there is a huge difference between sexual violence and consensual acts of bondage. There was also concern from young people who identify as LGB and T that some of the porn they can relate to might be labeled as “extremist” whereas in fact porn involving, for example, trans* individuals often reinforces their identity and sense of self, rather than being fetishistic.

Addressing the issue at the source

2.4 Some of the young people that Brook spoke with also felt that responsibility should be placed on the websites which host extreme materials. Rather than being an issue of filters, the issue should be addressed at the source.

“Surely the issue should be with the websites themselves existing, rather than blocking out young people’s free will to surf the web. We should be tackling the websites themselves, rather than blocking access to them...” Young person, 20.

“Make the promotion and creation of website such as these illegal and ensure that it’s an offence that the police take active force to enforce.” Young person, 23.

2.5 Furthermore, Brook and FPA would like to point out that although online pornography will almost always show consenting adults, it rarely shows that the consent leading to the actions being undertaken has been pre-discussed and negotiated. This leads to a perception that it is somehow acceptable to quickly engage in sexual acts that others may find extreme, without gaining the permission of all parties involved. Brook and FPA recommend that the perception of this needs to change, and the Government should implement policy which leads to pornography websites showing the consent and negotiation that leads to the sexual acts which are shown.

3. How best to prevent abusive or threatening comments on social media?

“Educating young people about how some people on the internet use anonymity and personas to try to hurt or control other people; and how to identify spaces in which they feel safe and unsafe so they can find spaces on the internet that suit them best. I would also foster a society in which people didn’t feel they needed to use the internet (or anything else) to dominate others, but that would take a while.” Young person, 24.

3.1 Brook and FPA concur with the views of the young people interviewed by Brook that cyber bullying should not be looked at in isolation, and that it is just one facet to the much wider issue of bullying generally. The solution is not as simple as increasing blocking or reporting options. What is really required is a societal shift in attitudes around respect and how we treat others. The media, in all its formats, has an important role to play in this shift, particularly in enforcing a message that there are no unhealthy sexual or societal norms that young people should feel that they should have to live up to with regards to their sexuality and sexual behaviour.

Helping young people to understand abusive and threatening behaviour

3.2 Further to our response to Question 1, Brook and FPA firmly believe that quality SRE as part of PSHE should encompass education that helps pupils understand why people bully, and to teach them to react in a way that is both responsible and appropriate to their individual circumstances.

“Teach the children to be understanding of the harsh semiotics of the internet, and how to be emotionally resilient and secure.” Young person, 18.

“You need to teach children to take advantage of the ability to block people on websites and use high privacy settings.” Young person, 18.

3.3 The young people that Brook spoke with also suggested targeting the bullies or potential bullies and increasing understanding of power dynamics through education.

“If you want to solve society’s problems, you need to start at the source.” Young person, 16.

“Education is key. Having the appropriate education at school will help people realise that being a keyboard warrior is not constructive.” Young person, 20.

3.4 As mentioned in our response to Question 1 under the “SRE and the prevention of sexual abuse, sexual exploitation and domestic and sexual violence” section, teaching about abuse has the potential to help both the perpetrators and potential victims of bullying and abuse. Brook and FPA strongly recommend the need for quality SRE as part of PSHE education to be fully implemented across all school settings.¹⁰²

The need for a transparent internet culture

3.5 The young people that Brook spoke with, described some innovative ideas about having more transparent internet culture, where websites should have clear terms of reference, including whether the website allows free speech, which some people may find offensive. Where “free speech which some people may find offensive” is endorsed, users of these websites should therefore be prepared for the fact that others can say what they like; or whether it is a friendly and respectful community, where people will be removed if they post something that is offensive. The obvious benefit of implementing such a system is that young people would be enabled to exercise choice over what type of online community they choose to be part of.

3.6 The young people also highlighted the importance of social media sites developing smooth mechanisms to ensure that trolls are dealt with quickly and appropriately. One young person suggested that in addition to trolls being blocked from social media sites where they demonstrate abusive behaviour, large fines could also be introduced in order to reinforce the anti-bullying commitment.

“Introduction of a procedure allowing anonymous trolls/abusers to be reported to either the website administration or the police.” Young person, 18.

“Sufficient justice for trolls, better functioning ‘flagging’ on social media sites”. Young man, 20.

Whistleblowing button

3.7 In addition to the need to report trolls and bullies, some young people that Brook spoke with also felt that more could be done to support children who do find distressing or extremist images online, and one particularly helpful idea was to enact a help/whistleblowing button on websites so that children can be immediately directed to reputable professional organisations and get advice about what they have experienced.

“Have a number/email/button that they can get in contact with so that if they see something inappropriate they can tell someone with influence who can do the right thing and reassure the young person.” Young person, 20.

¹⁰² Unfortunately, SRE across the country is often weak. There is lots of evidence to substantiate this, but most recently in May 2013, an Ofsted report found that schools are failing children and young people by not meeting the set statutory guidance on SRE, but equally there is a lack of accountability surrounding SRE and PSHE generally, highlighted by there being no set curriculum to deliver, and poor assessment (Not yet good enough: personal, social, health and economic education in schools, Ofsted, May 2013).

YOUNG PEOPLE'S RESPONSE TO THE CULTURE, MEDIA AND SPORT INQUIRY INTO ONLINE SAFETY

BACKGROUND

The Culture, Media and Sport Committee have decided to investigate a number of aspects of online safety that are currently raising concerns, in particular:

- How best to protect minors from accessing adult content;
- Filtering out extremist material, including images of child abuse and material intended to promote terrorism or other acts of violence;
- Preventing abusive or threatening comments on social media.

Brook will be submitting a written response to the inquiry where we will pull together recent policy and lines on the issue. Young people's views will form a key element of this response.

METHOD

In order to ensure that young people's views were accurately represented in Brook's response to the CMS inquiry, the Participation Lead created an online survey, which was promoted via our BeSexPositive social media channels, and asked groups of young people across the country to consider their views of the questions and themes raised in this Inquiry.

These groups included young people who identified as LGB and T (Lesbian, Gay Bisexual and Transgender), male, female and non-binary, BME (Black, Minority, Ethnic communities), experience of mental health, experience of homelessness, and as young offenders.

FINDINGS

Question 1: Some internet sites, for example those that show graphic images of sexual violence, are usually considered as inappropriate for young people under the age of 18. What do you think are the best ways to protect children, or younger young people, from accessing images that they might find distressing?

The young people were really clear that there needs to be a distinction between protection and censorship. They felt it was important to recognise the fact that some young people will be purposefully seeking out porn for a variety of reasons, including being intrigued about sex.

They felt that parents need to take responsibility for supervising their children and setting appropriate safety settings if they have young children who may be vulnerable to seeing images that they might find distressing. The young people pointed out that there are existing safety settings which are very good filters. They felt that if safety settings are used appropriately then young people would not come across adult content when searching for something else.

"Educate the parents, who can in turn educate the children." Young person, 18.

To enable parents to act accordingly, they suggested that education should be provided to parents so that they are able to understand and set parental controls. The young people we spoke to all knew how to do this themselves, describing the process as simple, and felt that there should be no reason why children should see adult content if they don't want to.

"We don't need to create new filters, we just need to educate parents about how to use existing safety settings." Young woman, 16.

They suggested developing leaflets, posters or training/workshops for parents, explaining how simple it is to set these controls.

"I think to help keep children from accessing images which may cause distress, parents and carers need to take responsibility to discuss these subjects with their children and as well as the need to make sure these kind of sites are not accessible if they have children under 18." Young person, 15.

They also felt strongly that young people should be taught about internet safety in school and taught how to set controls themselves. They suggested that educators could explain to children that there are image on the internet which may not be suitable, talk to them about what it means, and teach them how to avoid it. They thought that children should be taught that there are some things on the internet that they may find disturbing and that there are people they can talk to, if they do see something that upsets them.

"I think education is more important than sheltering young people and just pretending they are not there, because they would no doubt find them anyway." Young Person, 18.

"Better education in schools. Explain to them that those films are not real, and are actors." Young person, 20.

"Making young people and parents aware of how to block distressing images and educating children and younger young people about who to speak to if they come across something they find upsetting." Young person, 24.

“Educate parents on how young people access what they do and make it so that young people know that they can talk to their parents or someone they trust if they have seen something that makes them distressed.” Young person, 20

“I think educating young people on the different types of images etc is also important to ensure that when they are faced with such things they know how to deal with them.” Young person, 23.

Some young people also gave suggestions about how safeguards could be improved to ensure that children are not able to access adult content.

“Require date of birth confirmation before entering, have captions preceding these images warning of graphic content.” Young person, 21.

“Ensuring that there’s better parental controls, rather than just having to click a button to say you are over the age, instead asking the parent to enter the password. I also think that there should be better control over sites use of pop-ups and advertising on other websites that are harmless and have nothing to do with porn.” Young person, 23.

Question 2: What ways do you think would be best to protect children and young people from extremist material, such as images of child abuse and sites that promote terrorism or other acts of violence?

First of all, the young people thought it was important to give consideration to what is considered extremist. They were clear that images of child abuse or bestiality should be banned, but some felt that censoring images of bondage, for example, is wrong because it may be consensual. They were clear that there is a huge difference between sexual violence and consensual acts of bondage. There was also concern from young people who identify as LGBT that porn that they can relate to might be labelled as “extremist” whereas in fact porn involving trans* individuals often reinforces their identity and sense of self, rather than being fetishistic.

Again, the young people highlighted the importance of open and honest discussion, and comprehensive education, to inform children of the dangers of accessing certain sites, and the importance of education for parents to enable them to have those potentially difficult discussions, whilst also learning about how to use appropriate parental controls.

“I believe [that the way] to truly protect children from extremist material... is [by having] positive shared discussion, with family, carers or teachers when possible, about the subjects.” Young person, 15.

“Individual guidance by parents to ensure children don’t find this material. If a parent is present, even if they do find it, it can be explained properly, explained why it’s wrong and why not to go back to the site.” Young person, 18.

Some of the young people also felt that responsibility should be placed on the websites which host extremist materials. Rather than being an issue of filters, the issue should be addressed at the source.

“Surely the issue should be with the websites themselves existing, rather than blocking out young people’s free will to surf the web. We should be tackling the websites themselves, rather than blocking access to them...” Young person, 20.

“Make the promotion and creation of website such as these illegal and ensure that it’s an offence that the police take active force to enforce.” Young person, 23.

Some young people also felt that more could be done to support children who do find distressing or extremist images on line.

“Have a number/email/button that they can get in contact with so that if they see something inappropriate they can tell someone with influence who can do the right thing and reassure the young person.” Young person, 20.

Question 3: What do you think are the best ways that young people can be kept safe from abusive or threatening comments on social media? If you were in charge, how would you deal with internet trolls?

There was a strong focus from young people that cyber bullying should not be looked at in isolation, and that it is just one facet to the much wider issue of bullying generally. They felt that the solution is not as simple as increasing blocking or reporting options, and that what is required is a societal shift in attitudes around respect and how we treat others.

They suggested that all children and young people should receive education about relationships so that they can understand bullying and why people bully.

“Teach the children to be understanding of the harsh semiotics of the internet, and how to be emotionally resilient and secure.” Young person, 18.

“You need to teach children to take advantage of the ability to block people on websites and use high privacy settings.” Young person, 18.

They suggested targeting the bullies or potential bullies and increasing understanding of power dynamics through education.

"If you want to solve society's problems, you need to start at the source." Young person, 16.

"Education is key. Having the appropriate education at school will help people realise that being a keyboard warrior is not constructive." Young person, 20.

They also described some innovative ideas about having more transparent internet culture, where websites should have clear terms of reference, including whether the website allows free speech, and therefore people need to be prepared for the fact that others can say what they like; or whether it is a friendly and respectful community, where people will be removed if they post something that is offensive. Then young people would be enabled to exercise choice over what type of online community they choose to be part of.

"Educating young people about how some people on the internet use anonymity and personas to try to hurt or control other people; and how to identify spaces in which they feel safe and unsafe so they can find spaces on the internet that suit them best. I would also foster a society in which people didn't feel they needed to use the internet (or anything else) to dominate others, but that would take a while." Young person, 24.

They young people also highlighted the importance of social media sites developing smooth mechanisms to ensure that trolls are dealt with quickly and appropriately. One young person suggested that in addition to trolls being blocked from social media sites where they demonstrate abusive behaviour, they could also impose "large fines!" to reinforce the anti-bullying commitment.

"Introduction of a procedure allowing anonymous trolls/abusers to be reported to either the website administration or the police." Young person, 18.

"Sufficient justice for trolls, better functioning 'flagging' on social media sites". Young man, 20.

Question 4: *The Government is worried that children and young people can find porn too easily. What do you think? And if you were Prime Minister what would you do?*

"I believe if the Government feel the porn is too accessible and want to ensure young people don't see it, they should improve the sex education in schools. As porn is usually viewed by young people who are not entirely sure or can't understand sex, are intrigued to see what people do when they have sex (as this is not the kind of information we find out in sex education, we tend to only get the 'mate and fertilisation' and how to avoid becoming pregnant) especially LGBT youth. If I was prime minister I would insist more in depth sex education and awareness about LGBT sexual relationships." Young person, 15.

"I think it is more to do with education, I accessed pornographic images from the age of 11 and this was a lot to do with my own questions about my body and sexuality, but I was never given any outlet or information about these images, it was just not talked about at all throughout education[...] When children start to hit puberty then without places where they can talk about sex in a positive way (and not just mechanics) then they will go looking for potentially harmful images, and in the world we live in it is virtually impossible to censor those completely." Young person, 18.

"Mandatory relationship education that rolls on into sex education from a VERY young age." Young person, 18.

"Porn is not always a negative thing. Masturbation feels good; I enjoy watching porn when I masturbate... who are the government to intervene? If the government continues to speak about porn in this way it's steering us away from the goal of sex being more openly discussed in society. Look at the media...all of these over sexualised adverts and graphic scenes in films—blocking porn sites is a waste of time, instead they should be regulated; and young people should learn more about porn in schools." Young person, 20.

"If young people want to access porn, out of arousal or curiosity, that's perfectly healthy and typical. However, easy access to porn needs to be supplemented with good sex education and lessons about internet awareness and safety, as well as an open and non-judgemental societal attitude towards sex and sexuality." Young person, 24.

"I think there is imagery that could be considered pornographic everywhere (advertising, newsagents, etc) I think that the focus should be on educating children and young people about sex and parents essentially doing their job of parenting." Young person, 21.

"Enforce education. The sex ed bill hasn't been updated since 2000, predating all internet issues. This would be a cause for outrage in any other subject." Young man, 20.

"I would leave the porn industry as is. They already have age warnings on websites, many programs can be installed by parents that automatically block these websites (without infringing on adults and young people exploring their sexuality). Porn is labelled as 18+, but it's undeniable that many teens watch porn and watch it safely. For many people it's a major way of exploring their sexuality, being sexually satisfied and learning about themselves in a safe environment with no chance of disease and if they find a problem they just need to hit the close button." Young person, 18.

"I think that it's more important that young people receive better sex and relationship education in school to ensure that they are appropriately informed that porn is not reality and to help them understand what real sex and relationships look like." Young person, 23.

CONCLUSION

In conclusion, it is clear that the young people we spoke to demand better, more inclusive education on internet safety, both for children and for parents, to ensure that knowledge, skills and understanding around online safety are embedded in the next generation. This would support a societal shift in the bullying culture which has developed around social media, without imposing enforced censorship which could inhibit young people's ability to access accurate information about sex.

Compulsory education on internet safety, covering issues which include pornography and cyber bullying, would allow young people to explore and understand their developing sexuality whilst reducing any risk of harm.

September 2013

Written evidence submitted by Michael J Smaldon

I am writing this in my personal capacity as 1) a concerned father and 2) a Christian.

1. I am greatly supportive of the Government's inquiry into On-line safety, especially as far as children are concerned, and the proposal of an "opt-in" as being the default mechanism for accessing adult material on the internet.
2. I and my family have access to the internet, but only via a whitelisted secure access, and I am very concerned to understand that only 46% of parents have on-line filters.
3. I would strongly support an opt-in strategy as far as access to adult material is concerned, and I would encourage the Government to make this a rigorous and specific double check request so that applicants are under no misunderstanding as to the potential nature of the material that may be accessed.
4. We need to be jealous to maintain the simplicity and innocence of childhood, and the weak, and be aware of the very real dangers available one click away on the internet. We need to protect our young people, who are our future and our potential, from the morally degrading and dangerous aspects of the internet.
5. We also need to do everything possible to protect each and everyone of us from the corruption and danger which is rife and so easily accessible, and a specific double or triple block or check would also protect adults from moments of inconsidered and unwise access, which they will have cause to regret.
6. Moreover violence and pornography have had a very significant impact on family life, resulting not only in the breakdown of the family unit, but the scars of exposure are hard to heal, and the cost to the public purse in the cost of social breakdown in human terms, broken homes, social services, the NHS and charitable agencies is incalculable.
7. The internet can be a source of good information and positive interaction, but it verges too closely on the unacceptable, degrading and corrupt. Human nature being what it is, by its very character is easily tempted and corrupted; we cannot afford to allow this for ourselves, and if we have any appreciation and care for all our children, it is a responsible move and the only right step to ensure that they are not damaged by default.
8. An opt in, if you must, should be most deliberate and secure, and not easily overridden.
9. There needs to be action at all points of the Internet, 1) a secure and vigilant Ofcom with authority to monitor, moderate, and insist on compliance 2) A code and rules for social media that protects minors, and limits obscene material, and other inappropriate content 3) a triple part lock or opt in strategy which specifically and deliberately warns of potential content, likely effect, with a confirmation that persons still wish to access this area of the internet, and a Government warning that this will be detrimental to physical and moral health and wellbeing, with resultant risk being the full responsibility of the person concerned.
10. It should not be possible to access such information under any circumstances by mistake.

I should like to thank the Committee for their consideration of this matter, and commend them for having the interests of our young people at heart. We pray that you will be strengthened to bring this matter into law, in the understanding that "evil communications corrupt".

September 2013

Written evidence submitted by Prof Andy Phippen

CONTEXT

I have been involved in research around online safety for over 10 years and work very closely with organisations such as the UK Safer Internet Centre and South West Grid for Learning as well as many schools across the country. This work, over the years, has encapsulated issues of identity and trust, school policy and practice around online safety, online safety problems faced by children and young people and how our understanding of these have changed over the years, and the impact of new technologies on behaviours. I work with young people from primary age up to higher education.

In all of my research a fundamental aspect is being able to discuss these issues at a grass roots level with young people themselves. While we might have additional data collection mechanisms such as survey work, the core of any research project will be sitting with young people, usually in groups, talking about the research questions and their thoughts. This is all conducted within a clear ethical framework working alongside schools to place the young people in a safe, non-judgemental environment where they are free to share opinions and reflections without being challenged or confronted. Parental consent is obtained for any young people spoken to, they are fully briefed on the research context, and have the right to withdraw from the discussions at any time. While these discussions can sometimes centre on difficult issues, such as sexting, pornography and gender, I usually find the discussions very open and productive (we don't ask young people to disclose about their own behaviour, but to reflect on the behaviour of peers). I also work with stakeholders in the online safety area, such as parents, teachers and social care professionals to understand their attitudes and concerns related to online safety and young people. A recent example of this work was a piece of research conducted by the NSPCC/UK Safer Internet Centre around sexting.¹⁰³

In addition to research practice, I am also involved with a lot of schools in an educational context, delivering assemblies and classes related to online issues and associated behaviours. While this is not formal research work it further allows the exploration of online safety with young people in a qualitative setting and can elicit interesting and rewarding discussions.

As well at the work above, all of which is available in the public domain, I am currently involved in three qualitative studies that, while not yet published, may have relevance to this inquiry. These studies are:

- An exploration into gaming culture and its impact on behaviour and attitudes.
- Research into gender imbalance and issues around sexist abuse and the role online technology plays in facilitating these.
- Exploring the impact of superfast broadband on young people's use of online technologies.

In presenting a response to the CMS Committee Inquiry into Online Safety, I will draw from all of this work to place context around my responses.

Clearly the online world is something with which the vast majority of young people are engaged and use on a daily basis (indeed, the differentiation between the online and offline is often something young people do not acknowledge, it is simply "life"). In agreement with the specified inquiry brief, one thing I can observe through many years working in this area is that public understanding of the issues involved in "being" online has improved and we have moved on from the traditional threats such as "stranger danger" to a realisation of a complex environment requiring multi-stakeholder input and perspectives. In addition, within the field we have moved away from the belief that young people are simply passive participants needing protection toward an awareness of fully engaged digital citizens who need to be mindful of the impact of their own behaviours on others as well as awareness of the risks involved living in the online world.

Digital risk can take many forms, from those well established such as grooming to sexting, cyberbullying/online abuse, accessing inappropriate content and trolling. However, in ensuring protection from harm we must also establish a balance with rights to freedom of expression and access to legitimate content and interaction.

As someone who has worked in the field for a long time, it is encouraging to see Parliament engaging with these issues in recent time. However, a lot of recent policy discussion around this topic has focused on a very specific aspect of online life—access to adult content and the measures needed to ensure young people cannot see this.

More concerning is that this dialogue seems now to have grouped access to clearly illegal content (child abuse images) with access to legal content for adults which is inappropriate for minors. These are two very separate issues and it is not helpful to be presenting them in the same context—countermeasures to tackle child abuse images are clearly set in law and addressed by excellent organisations such as the Internet Watch Foundation. Child abuse images are illegal and no one has the "right" to access them. However, when we are talking about legal content inappropriate for young people it is a far more complex debate as we do not want to restrict the rights of the public or ostracise them in some way (for example by suggesting that there is a link between access to legal and illegal content) in order to protect young people.

This is a very narrow aspect on online safety at large—what about sexting, cyberbullying, trolling, upset by "innocuous" content, education, the right to discuss these issues in school, etc? It is encouraging to see that

¹⁰³ http://www.nspcc.org.uk/Inform/resourcesforprofessionals/sexualabuse/sexting_wda93252.html

this inquiry is, at least in part, looking to broaden to Parliamentary debate and to start to ask questions around the wider context. This is something that will be explored in more detail when addressing the specific points of the inquiry below.

HOW BEST TO PROTECT MINORS FROM ACCESSING ADULT CONTENT

There has been much discussion over this point over the last couple of years. The OCC published an excellent, balanced, review of the literature in this area recently.¹⁰⁴ However, I would like to present a slightly different perspective on this matter that has arisen from my discussions with young people. Adult content is certainly nothing new, it has been available far longer than it has been accessible online. However, the challenge presented in the online world is both accessibility and the type of content one can now download. While 25 years ago magazines and perhaps VHS videos provided a level of access to adult content, it was not as strong or diverse at the availability of pornography online. This is something that has been acknowledged by many young people I have spoken to.

I was asked over the summer this year by a 14 year old boy what I thought about people his age looking at this sort of content. This is an interesting question to pose because it both acknowledges that young people of this age are frequent users of pornography (this has been borne out in my discussions with young people of this age, particularly boys) and also challenges the social belief they should not be doing it. My answer was hopefully a pragmatic one—I would rather they didn't but I wasn't naïve enough to think they could be prevented from accessing it, so I would rather we focused on providing an environment in schools where they could talk about the possible issues that arise from access to this sort of content.

Protection from access is an interesting concept. How can we protect them from content they wish to access (which is certainly something I would observe from talking to boys far more than girls)? This, again, was reflected in discussions recently with a very mature group of 14–16 year old boys in a local school—one boy, who was discussing the recent policy discussions around “opt-in” and filtering in the home, made a very clear statement: “You will not prevent teenage boys from accessing pornography”. He did not state this to be rebellious or controversial, he was stating it from his observations of his peers. They access and share pornography and have many ways of doing so.

Much of the recent debate has been around filtering and it is worth exploring this as a “solution”, which is clearly is not. Software can only ever provide tools to provide some level of support to what are, essentially, social issues facilitated by technology. We have worked with filtering in schools for a long time now and while it is certainly a useful tool to prevent access to inappropriate content in the school setting, it is equally clear that filtering controls have to be set extremely high in order to prevent access to those things the school does not wish their pupils to see.

Therefore, lots of innocuous content will be also be blocked which can lead to frustration for both staff and pupils. This is because filtering is still a pretty blunt tool—in general it looks for keyword and blacklisted sites and prevents access as a result. Filtering still struggles with context—the famous Scunthorpe problem being a clear example of this (and some filters will still block this). Filtering also only blocks the channel on which the technology is installed—in the case of a school this channel would be the institutions network. It will not prevent an ambitious young person with a mobile device handed down from their parents from accessing this content. And if an individual's mobile device has been set up to prevent accessing adult content, they will have a friend whose device hasn't and they will share content via Bluetooth, MMS, etc.

One boy I spoke to recently was more candid when I discussed the recent policy directions with him—he said he doesn't care whether people prevent him from accessing indecent images online, he'll just ask a local girl to send him pictures instead. While this does present a number of issues, notwithstanding a very concerning attitude toward women in general, it does clearly highlight one issue that doesn't seem to be discussed in the recent debates—online consumption of “professional” pornography is only one source of indecent content for young people.

Filtering will prevent access for those not wishing to find inappropriate content, and as such does provide some use in this area. If we turn our focus to filters in the home it may prevent younger children from stumbling across this sort of content, but will it “protect” a determined teen? Also, if filtering in the home is going to present similar overblocking challenges as those solutions in schools, how many homes will switch off the filters because they become too frustrating to use and because they prevent access to legitimate content? Certainly the Open Rights Group (I am on the advisory council for this organization) have many examples of adults contacting them because of filters that, whether on home computers or mobiles, have prevented access to legitimate sites with no means to unblock them.

On countless occasions young people have asked me why they have no opportunity to discuss these issues in school. Many are also critical of what learning they do have around online issues in either PSHE or sex education. Rather than just trying to prevent young people from accessing these sort of things, which will always be a game of catch up when they are finding new ways of access, should we not be providing an education environment where these issues can be discussed? Shouldn't we be providing a means for reflection and challenge on why society feels this content is inappropriate for young people and what the impact of

¹⁰⁴ <http://www.mdx.ac.uk/Assets/BasicallyporniseverywhereReport.pdf>

access might be? Sex education which addresses online issues, inappropriate content, etc, seems to be extremely disjointed and generally delivered by the few specialists we have in this area in the UK. I certainly hear very rarely of this sort of lesson being delivered in a school by teachers within the establishment. Yet whenever I have had sessions in schools with both boys and girls around this topic (which can result in very different conversations) I have found the young people to be engaged and enthusiastic in their discussions and ask to do more of this sort of thing.

So the barrier is not the unwillingness of the pupils, but the lack of coordination nationally to permit teachers to address these things in schools. Education in this sort of area requires multi-stakeholder buy in from staff, parents, pupils and policy makers. A lone teacher who believes this is important may subsequently suffer at the hands of senior management, parents or governors who have received no “permission” to address these topics within the curriculum.

FILTERING OUT EXTREMIST MATERIAL, INCLUDING IMAGES OF CHILD ABUSE AND MATERIAL INTENDED TO PROMOTE TERRORISM OR OTHER ACTS OF VIOLENCE

Much of the discussion above is equally pertinent to this point, filtering cannot be seen as the complete solution. It is good to see acknowledgement that harmful content online is not just pornography (indeed, in my discussions, young people are far more likely to say they have been upset by images of violence or animal abuse than they are by sexual content) but again we need to be clear about the difference between what is legal and what is illegal. If content is illegal, the Internet Watch Foundation (IWF) have a very clear remit for reporting, investigating and either blocking or moving for prosecution (depending on whether the content is hosted abroad or in the UK). The IWF maintain a blacklist of sites serving illegal content and all ISPs within the UK buy into this. The key challenge for the IWF is awareness of their role among the public and this could be something that could be helped by UK Government.

However, when we consider legal, but upsetting, content, we are in more difficult territory if we are looking to filtering as a solution. Who decides what should be filtered? How can we be sure about the meaning and intent behind a search term (for example, if one is searching for extremist materials might use the same search terms as someone conducting research on the area)? And is this a sliding scale of upset? I have had many young people tell me how RSPCA adverts have upset them—should we move to block them too? Again, I would rather see a society that, rather than trying, and failing, to prevent access to anything that *might* upset a young person, provides an environment where there are aware upsetting content can come in many different forms and affect individuals in different ways and if they are upset, they can talk to someone about it. During my work around sexting I was amazed at how few young people would turn to a teacher if they became a victim. They feared a lack of understanding or a judgmental response. That is a real concern because we cannot possibly consider, and filter, all content any individual young person might find upsetting. To consider young people as a single collective is patronising to the diversity and individuality they exhibit and what upsets one may be viewed as humorous or innocuous by another.

PREVENTING ABUSIVE OR THREATENING COMMENTS ON SOCIAL MEDIA

Finally, while it is good to see an Parliamentary committee looking at this issue, because when I talk to young people about online issues cyberbullying (or simply “people being mean”) is by far the most likely response when I ask what upsets them online, I would, again, take issue with the wording used. Put simply, you will never *prevent* abusive or threatening comments on social media, just as you will never prevent nasty comments in the playground, on TV shows such as the X Factor, on the football pitch or at PMQs. However, far more can be done to provide an environment where young people should know they do not have to put up with this sort of thing and that people can help. I should stress, first of all, that it is rare that a young person will talk about “cyberbullying” and the term is unhelpful when trying to address the problems caused by people being abusive online. Online abuse can be described in many forms, such as nastiness, people being mean, calling names, ganging up or simply banter and again equitability is difficult to manage in this area—one young person’s banter will be considered abuse by another.

However, it is important that services providers offer the means to report abuse, something that is already in place by some social media platforms but not others. Young people also need to be aware that they can use these reporting mechanisms to take comments down and also they will not get into trouble themselves. The wording of some reporting functions is intimidating and can be overwhelming for young people.

But, once again, education is the pivotal player in this area—education around what is and isn’t acceptable language, the impact of abuse on others, the disconnect and perceived anonymity the Internet provides, and the potential illegality of some forms of abuse.

It is also encouraging to see some discussion from the Director of Public Prosecutions and Crown Prosecution Service around this issue, it is helpful to get some clarification on abusive language. It is also encouraging to see it stated it is rarely in the public interest for minors to be prosecuted for this sort of thing.

I have seen a number of schools adopting a restorative justice approach to the resolution of online abuse issues and this makes sense—in a lot of cases the perpetrator will not be aware of the impact of their words on the victim and to place them in an environment where they can hear about it is a powerful one. However,

it is important the restorative justice is implemented effectively with trained counsellors—it is not something that can be done effectively without experienced professionals.

In summary, it is encouraging to see this inquiry exploring some of the broader issues around online safety and not just focus on the headline grabbing ones. However, it is still a concern that a lot of the language focuses on prevention and filtering rather than education and awareness. The Internet is not something that can be “policed” with technology. If we wish to protect young people and help them protect themselves, we cannot lay responsibility solely on service providers and software just as we cannot blame the Royal Mail for delivering an unwanted letter. We need parents to be aware of issues, we need education professionals to be able and allowed to provide an effective environment to both learn about and talk about these issues, and we need policy makers who are awareness of the broad context of online safety and the complexities of growing up in the digital age.

September 2013

Written evidence submitted by the Ahmadiyya Muslim Community UK

INTRODUCTION

1. We welcome the opportunity to provide evidence to the Culture, Media and Sport Committee as it considers its inquiry into online safety. This submission is on behalf of the Ahmadiyya Muslim Community UK. Members of the Ahmadiyya Muslim Community are subject to various forms of discrimination, violence and persecution in a number of countries around the world.

2. There is an increase of cases within the UK, where extremists are now using media such as online websites and television programmes to promote their extremist views to members of the public in the UK. There have been many cases where in turn this has led to discrimination and promotion of hatred in the UK against the Community.

3. We would like to take the opportunity to make representations in relation to extremist material, including material intended to promote hatred, terrorism or other acts of violence on the internet and also in relation to preventing abusive and threatening comments on social media.

4. This submission focuses on some illustrative examples of such material, and makes a number of recommendations. Further details giving the background of the Community can be found in the annex to this submission

ISSUES ABROAD—CASE STUDY: PAKISTAN

5. As is well known, the internet is a global phenomenon that transcends national boundaries, and as a consequence also transcends national laws. The implication of this is that whilst historically, extremism was contained within national boundaries and national legal systems, modern trends of extremism transcend those historic constraints through the internet, including through social media. As a result, extremism in one country of the world can now be directly targeted and have direct effects on individuals and communities in other parts of the world.

6. In order to explain the range of issues faced in the UK predominantly through extremist material online, this submission will look at the example of Pakistan and how extremists are now using material online to infiltrate extremist views here in the UK.

7. The persecution faced by the Community and its members in Pakistan is well documented and has been entrenched within the Pakistani state and society for decades. A brief overview of the effects of this persecution and discrimination is outlined in Table 1 below.

Table 1

PAKISTAN PERSECUTION STATS: 1984 TO DEC 2012

| | <i>Number</i> |
|---|---------------|
| Ahmadis Killed | 226 |
| Ahmadiyya Mosques Demolished | 24 |
| Ahmadiyya mosques sealed by the authorities | 28 |
| Ahmadiyya mosques set on fire | 13 |
| Ahmadiyya mosques forcibly occupied | 16 |
| Ahmadiyya mosques, construction barred by the authorities | 46 |
| Ahmadi bodies exhumed after burial | 35 |
| Burial of Ahmadis was denied in common cemetery | 58 |
| Ahmadis assaulted for their faith | 175 |

8. In Pakistan, members of the Community are legally prohibited from calling themselves Muslims, cannot engage in any Muslim rites and practices, cannot vote, and cannot speak in defence of their faith in the media.

In particular, the Community and its members are declared “wajbul qatl” (deserving to be killed) publicly by clerics with no one—the police, media, government, nor the military—willing to defend the Community and its members from the extremists.

9. The persecution of the community in Pakistan is a case of the politicisation of religion by extremists. Legislation has entrenched the persecution and discrimination of the Community and its members in law. This has emboldened extremists (for examples groups such as the Majlis Ahrar, the Jamate Islami and the Majlis Khatme Nabuwwat) that have used these laws as a pre-text to discriminate, attack and kill members of the Community in Pakistan.

10. As a result, in Pakistan, extremists have had an open hand and regularly transmit or publish hate messages, death threats and even hit lists of members of the Community declaring that killing of an Ahmadi is a noble act (for example, such lists were distributed openly in Faisalabad in 2011).

MATERIAL INTENDED TO PROMOTE TERRORISM OR OTHER ACTS OF VIOLENCE

11. The significance of this situation faced by the Community and its members in Pakistan is twofold. First, given the global nature of the internet, the extremism that has been entrenched in Pakistan (and indeed in other places in world) now has a foothold to spread across the world, including in the UK. Second, some of the large Pakistani diaspora in the UK has, at best, sympathies with these extremist views, and at worst, is encouraging and promoting these extremist views in the UK.

12. There is, at present, no specific regulation governing content on the internet. This lacuna is allowing a range of groups to successfully advocate their extremist views, including to audiences in the UK.

13. At present, the only scope for targeting such extremist material online in the UK is prosecutions under The Racial and Religious Hatred Act 2006. Part 3A of the Act states that “A person who uses threatening words or behaviour, or displays any written material which is threatening, is guilty of an offence if he intends thereby to stir up religious hatred.”

14. Although it would appear that any threatening written material would be governed by this provision, the Crown Prosecution Service (CPS) has been limited in its ability to prosecute such incitement to hatred on the basis of the present laws. Additionally sometimes when a potential breach comes to light, the offender withdraws it from the internet and it can no longer be traced for prosecution purposes. But his damage has been inflicted and there is no remedy against this.

15. In order to successfully prosecute under the law for acts of hatred there is a two limb test. Firstly, whether the accused incited and secondly whether the accused had the necessary intention to incite. The first test is nearly always fulfilled however it is the *intention* that is extremely difficult to prove. The consequence is that whilst clear incitement is made out, the threshold to prosecute is not fulfilled.

16. Whether or not through criminal laws, there is a clear need for online regulation to be enforced to prevent the dissemination of extremist material promoting hatred and leading to violence. Due to the lack of any such regulation, extremists groups are finding it an easy location to promote their material. This in turn is having a direct effect on the Community and its members here in the UK.

EXAMPLES OF SUCH MATERIAL INCITING HATRED AND MURDER ONLINE

17. Various websites are deliberately promoting hatred online against the Community and its members, and have openly promoted the notion of “WajbulQatl” (deserving to be killed) as has been done in Pakistan.

18. A few examples of various websites promoting such online material are set out below.

- (a) www.madni.org/Qadiani/difference.htm

On this website it describes three types of “disbelievers”. Subsequently (extracted below) it is explained that *Muslims should kill an apostate*. It is further explained in the last screen shot that *Ahmadi Muslims* referred to as Qadianis are the third type of disbelievers and they *should also be killed*.

- (b) <http://www.paklinks.com/gs/all-views/405097-qadiani-ahmadi-population-in-pakistan-globally.html>

This is an example of a blogging site where it shows that it is now widely known among online users that Ahmadi Muslims should be killed.

- (c) <http://irshad.org/exposed/fatwas/edesai.php> and <http://irshad.org/brochures/message.php>

Inciting hatred and calling for a social boycott of Ahmadi Muslims.

19. The above examples are by no means exhaustive, but provide an insight into the many websites widely accessible on the internet, which are promoting discriminatory material and openly promoting violence and hatred online.

CONSEQUENCES OF DISCRIMINATORY ONLINE MATERIAL

20. The Community and its Members have faced direct consequences due to such and similar material published online. Posters and leaflets have been distributed inciting hatred and worryingly there have been cases where children have been able to access such material and bullied Ahmadi Muslim children at school.

21. Below are a few examples of such incidents:

- (a) <http://www.channel4.com/news/hate-crime-investigation-into-threats-against-ahmadi-muslims>

This news report by Channel 4 illustrates the use of posters explaining how the businesses of Ahmadi Muslims should be boycotted and one example of a member of the Community being dismissed from employment due to his religion. There is also mention of online videos on YouTube which also call for Ahmadi Muslims to be boycotted. Leaflets which are readily available online are also shown posted on shop windows.

- (b) http://www.khatmenubuwat.org/media/File/leaflets/mta_tv_eng.pdf

This link shows posters in shop windows calling for Muslims to be aware of Qadianis (Ahmadi Muslims). The poster displayed on that shop is readily available on the internet.

The poster states: "This notice is to serve warning that we should all be aware of the transgression by the Qadiyanis and not fall into their trap". It further calls on readers to make more copies of this poster and distribute it.

The hate campaign leaflet was also reported in local news:

- (c) http://www.yourlocalguardian.co.uk/news/8451668.Religious_hate_leaflets_found_in_Tooting_Streatham_and_Kingston/?ref=ar

http://www.yourlocalguardian.co.uk/news/local/wimbledonnews/8451429.Hate_campaign_discovered_against_Islamic_minority/

The above news report shows how leaflets have been posted in shops calling for the boycott of Ahmadi Muslim businesses.

22. Even at universities leaflets are being distributed which incite hatred against Ahmadi. As majority of these leaflets are made digitally it is extremely easy for such material to be made accessible online or to be distributed using the internet.

23. It is also well known that there has also been an increase in discriminatory content and promotion of terrorist views on digital television channels such as the Ummah Channel and Takbeer TV. Although the Committee is not investigating television safety, we believe that the importance of having stricter regulations is highlighted by some cases of discrimination and promotion of hatred on television.

24. The biggest difference between discriminatory and extremist materials online and on television is that the broadcast media is regulated by OFCOM. As such, OFCOM is able to investigate and address cases of extremist and discriminatory material that is broadcast. However, OFCOM has jurisdiction in UK borders and invariably surrenders supervisory control to overseas broadcasting regulators (even if such programmes are broadcast on the internet and can reach UK audiences) where different definitions and thresholds for what constitutes hatred and abuse may apply.

25. Below are two reports by OFCOM in relation to hate material against the Community and its members:

- (a) <http://stakeholders.ofcom.org.uk/enforcement/broadcast-bulletins/obb167/>

- (b) <http://stakeholders.ofcom.org.uk/binaries/enforcement/broadcast-bulletins/obb222/obb222.pdf>

26. OFCOM has since fined Takbeer TV £25,000 as they were found to be in breach of regulations: <http://www.media247.co.uk/bizasia/ofcom-fines-takbeer-tv-25000-for-verbal-abuse.105>

CONCLUSION

27. It is our view that it is evident that there is a serious issue that must be dealt with. Inaction at this stage will simply provide a blank cheque to extremists who wish to promote their hatred and violence in the UK, and allow discrimination and persecution to take root in communities in the UK. Material online needs to be subject to controls that prevent the promotion of discrimination, terrorism and other extremist views.

28. The limited examples set out in this submission are only a few such examples. However, what is plain is that where there is statutory regulation, authorities such as OFCOM have been better able to address this material.

29. There is no doubt that freedom of expression must be protected. Individuals and groups must be permitted to express their views and opinions, even where those views can be considered as critical and even distasteful by those against whom they are targeted at. Indeed, the Community and its members have no objections whatsoever to legitimate criticism and robust debate aimed at it and its views, and is always ready to welcome and engage debate and criticism.

¹⁰⁵ Despite this offence, the presenter hopped channels and committed the same offence but this time the new channel was able to put a stop to it.

30. However, where such views are expressed in a way that promotes discrimination, hatred and violence, they cannot be tolerated. Indeed, such speech is not protected by freedom of expression. It is necessary for the State to take robust action where such material is disseminated, in order to protect those who are the target of such discrimination.

31. A possible range of options open to the State might be:

- (a) Establish a statutory regulatory body (such as Ofcom) to investigate and take measures and sanctions against those promoting such material online (or extend Ofcom's powers to cover this function as well);
- (b) Establish a non-statutory body (such as the Internet Watch Foundation (IWF)) to investigate such material online, and notify ISPs to take measures against such websites;
- (c) Place a statutory obligation on ISPs to take action against websites disseminating such material online.

32. There are plainly advantages and disadvantages to these options (and indeed the wider range of options that may exist). These would need to be considered carefully by the Committee, and we stand ready to provide further evidence, as necessary.

33. It is our view that if the flow of extremist material is not halted then it feeds the process of radicalisation and poses a serious threat to community cohesion and the security of the UK. It is therefore in our national interest to take action on this important issue.

Annex 1

ABOUT THE AHMADIYYA MUSLIM COMMUNITY

1. The Ahmadiyya Muslim Community was established in a small village called Qadian, (Punjab, India) in 1889 by Hazrat Mirza Ghulam Ahmad who claimed under Divine guidance to be the Promised Messiah who had been prophesied in various world religions as well as the Imam Al-Mahdi of Islam.

2. His claim is unique in the Muslim world and his mission was to revive the true teachings of Islam that had become eroded over time. He brought no new laws or scriptures but emphasised the spiritual and humanitarian aspects of faith saying that Islam teaches man to love God and to love his creation and that Islam's true beauty lay in its powerful message of peace.

3. He advocated that true Jihad was an inner struggle for peace not a violent war against unbelievers as had been popularised by fanatic clerics. He also stated that religion and state were separate entities so the perception of the need for Sharia law to be imposed over the citizens of a country was unfounded in Islam. He noted that whilst Islam certainly offered guidance to God but the Holy Quran was clear that "There should be no compulsion in religion" (Ch 2: V.257).

4. After his claim to be the Promised Messiah and a Prophet (albeit one without a new law) he and his community faced strong opposition. That opposition in some cases has since grown into full-blown state sponsored persecution.

5. After his demise in 1908 the system of Khilafat ("Caliphate" or Spiritual Leadership) was reinstated. The Khalifa is elected by members of the community via an electoral college and the post is held for life. This has provided the community with leadership that is unique in the Muslim world. Due to persecution in Pakistan—where the Community had moved to followed the Partition of India in 1947—the fourth Khalifa migrated to the UK and the seat of the Khilafat has been based in London ever since. The current Khalifa is His Holiness Hazrat Mirza Masroor Ahmad who was elected to office in April 2003 as the community's fifth Khalifa.

6. The Community is established in 204 countries and has more than 100 branches across the UK alone. It works tirelessly for the wider community in which it exists with its work well known among the current government with the support of the Prime Minister, Deputy Prime Minister and the leader of the Labour Party. The Community is also well known for building London's first mosque (also known as *The London Mosque*). The community has also built the landmark Baitul Futuh Mosque in Morden, which is also the largest mosque in Western Europe.

7. For further information see www.alislam.org and www.LoveForAllHatredForNone.org

Written evidence submitted by the Sex Education Forum

SUMMARY

1. Technical solutions such as lessons about online safety in computing classes and internet controls are by themselves insufficient to protect children and young people. A broad and comprehensive programme of sex and relationships education (SRE) in school is essential to ensure that children and young people get accurate information about sex and sexual health and an understanding of what constitutes respectful relationships. This has been recognised in numerous reports including by Ofsted and the Office of the Children's Commissioner.

2. A broad programme of good quality SRE should also address the issue of on-line safety and pornography. This can complement the more technical learning about safety gained through computing classes.

3. Currently the provision of SRE in schools is unacceptably patchy and inconsistent. Every child and young person has a right to comprehensive SRE and we (as adults) have a duty to ensure this.

4. The best way to ensure this is by making SRE (within Personal, Social, Health and Economic (PSHE) education) compulsory for primary and secondary schools, and for teachers to receive training on the subject. The Government guidance on SRE should also be updated to provide clarity to schools.

5. The majority of parents want SRE to be compulsory in schools and many would also like support to fulfil their role at home as educators about growing up, safety, sex and relationships.

6. Our evidence submission to this inquiry covers:

- What is SRE and how can it address online safety?
- What is the standard of SRE in schools today?
- What is the evidence that SRE works?

What is SRE and how can it address online safety?

7. SRE involves learning about the emotional, social and physical aspects of growing up, relationships, human sexuality, sex and sexual health. It should equip children and young people with the information, skills and positive values to enable them to have safe, fulfilling relationships and to take responsibility for their sexual health and wellbeing.

8. Children and young people sometimes find pornography because they are looking for information about sex and relationships online. Further research is needed to establish if there is a link between good quality SRE and access/avoidance of pornography. Gaps in research about the link between accessing pornography and behaviour are identified by Horvath (2013) in the Office of the Children's Commissioner report "Basically...porn is everywhere". However, provision of good quality SRE means that young people have a reliable source of information about sex and relationships. Good quality SRE contributes to understanding how pornography distorts reality by discussing how media represents men and women and gender roles, and how pictures and videos are routinely edited.

9. The Sex Education Forum e-magazine shows how pornography and issues related to it can be effectively addressed in SRE and includes suggestions from pupils about the key messages that should be taught to their peers.

10. This is what a group of Year 11 pupils thought other young people should know about pornography:

About safety: Not all things shown in pornography are safe in your own sex life: keep safe, use condoms and go to a clinic regularly.

About privacy: No video cameras in the room! In case you film yourself but then have a bad breakup, keep your sex life private.

About reality: Don't believe everything you see. Pornography is acting and not "real". The sex and bodies are mostly unrealistic—and there is a lot of editing.

About the actors: Some people may be forced into making it. Some actors use performance enhancing drugs to "perform" or to be able to get through stuff that is painful. It can affect the actors physically, mentally and emotionally, and can mean that relationships suffer. There are dangers risked by the actors like infections and abuse.

About sex lives and relationships: You can learn some helpful positions from some films. The so-called pleasure you see may be anything but. You don't have to watch it at all. It can be addictive to the viewer and can mean that you might not be able to have a healthy, happy sex life yourself if you are addicted.

Always have consent: don't pressure people to do stuff from pornography or to watch it if they don't want to.

From "The Sex Educational Supplement" Issue 1 (2013).

11. At primary school classes should start with discussing differences between boys and girls bodies, and the importance of loving and respectful relationships. Learning correct names for genitalia is important so that

children have the language to describe their bodies, understand what behaviour would be abusive and report it if it happens to them. At secondary level lessons can look at “sexting” and pressures from peers and make more direct reference to pornography in the context of learning about consent, body image, gender roles and respectful relationships.

12. Having a basic universal language about respect, our bodies, growing up and sex is essential to support children with the words needed to report abuse and the belief that it is “OK to talk about this”.

What is the standard of SRE in schools today?

13. Ofsted inspectors report that SRE is currently inadequate in a third of schools (2013). Young people have repeatedly said that the SRE they receive is inadequate—with 28% describing their school SRE as “bad” or “very bad” in a survey in 2011 (Sex Education Forum). Young people say that the relationships aspect of SRE is the most neglected (Sex Education Forum 2008).

14. Ofsted consulted pupils for their recent PSHE report “Not yet good enough” (2013) and consequently recommended that schools address pornography within SRE. New research with young people carried out by Brook (2013 unpublished: also being submitted to this inquiry) shows that young people want young people need better, more inclusive education on internet safety, both for children and for parents, not least to ensure that knowledge, skills and understanding around online safety are embedded in the next generation.

15. Ofsted are also concerned that some primary schools are failing to teach the basic body science that is necessary to underpin further learning about bodily privacy and safety. They found: “*younger pupils had not always learnt the correct names for sexual body parts*” and see this as a safeguarding failure because it leaves children without the language skills to understand their bodies, know what is acceptable/unacceptable and to say what has happened to them (2013).

What is the evidence that SRE works?

16. National and international research shows that good quality SRE has a protective function as young people who have good SRE are more likely to choose to have sex for the first time later, more likely to use contraception and to have fewer sexual partners (Kirby 2007, UNESCO 2009 and NICE 2010).

17. A comprehensive programme of SRE also results in young people being less likely to have an “age-discrepant” partner (Lindberg 2012). Having an older partner is a significant risk factor for experiencing physical, emotional and sexual violence (for girls)—and a risk for sexual exploitation (Barter, 2009).

18. There is also evidence that SRE is more effective if home and school are involved (Kirby 2007 and see Emmerson 2011). Parents are overwhelmingly supportive of SRE and a recent survey shows that 83% of parents want SRE lessons to cover issues relating to pornography (NAHT, 2013 and see also Mumsnet 2011).

19. SRE aims to contribute to behaviour change, including reducing unprotected and unwanted sex, and reducing harmful behaviour, including sexual offences such as assault and abuse.

20. Good SRE, together with access to sexual health services will contribute to several public health priorities that are essential for the health and well-being of the nation, and especially to women:

- earlier reporting of sexual abuse and, in some cases, its prevention;
- reduction in intimate partner violence;
- reduced number of unplanned pregnancies;
- reduced maternal mortality;
- reduced infant mortality;
- prevention and earlier treatment of sexually transmitted infections; and
- reduced gap in health inequality.

REFERENCES

Barter, C, *et al* (2009). Partner exploitation and violence in teenage intimate relationships. London: NSPCC.209pp

Emmerson, L (2011). Parents and SRE: A Sex Education Forum evidence briefing, London: Sex Education Forum. http://www.ncb.org.uk/campaigning/media_news/2011/jan-jun/parents_want_support_with_sex.aspx

Horvath, M and others (2013). “Basically... porn is everywhere; A Rapid Evidence Assessment on the Effects that Access and Exposure to Pornography has on Children and Young People, Middlesex University London for the Office of the Children’s Commissioner”. <http://www.mdx.ac.uk/Assets/BasicallyporniseverywhereReport.pdf>

Kirby, D (2007). Emerging Answers: Research Findings on Programs to Reduce Teen Pregnancy and Sexually Transmitted Diseases. Washington, DC: National Campaign to Prevent Teen and Unplanned Pregnancy.

Lindberg, L and Maddow-Zimet, I (2012). Consequences of Sex Education on Teen and Young Adult Sexual Behaviors and Outcomes, in *Journal of Adolescent Health*, Volume 51, Issue 4, Pages 332–338, October 2012. [http://www.jahonline.org/article/S1054-139X\(11\)00717-8/fulltext](http://www.jahonline.org/article/S1054-139X(11)00717-8/fulltext)

Mumsnet survey of 1,000 parents (2011). <http://www.mumsnet.com/campaigns/mumsnet-sex-education-survey#Results>

National Association of Headteachers (2013). Research carried out in April 2013 by Research Now and commissioned by the National Association of Headteachers (NAHT) and press released by NAHT in May 2013. <http://www.naht.org.uk/welcome/news-and-media/key-topics/parents-and-pupils/parents-want-schools-to-manage-dangers-of-pornography-says-survey/>

NICE (2010). Public Health draft guidance; School, college and community-based personal, social, health and economic education focusing on sex and relationships and alcohol education. <http://www.nice.org.uk/nicemedia/live/11673/49240/49240.pdf>

Ofsted (2013). “Not yet good enough; personal, social, health and economic education in schools”, Ofsted, May 2013. <http://www.ofsted.gov.uk/resources/not-yet-good-enough-personal-social-health-and-economic-education-schools>.

Sex Education Forum (2008). Forum briefing: Young people’s survey on sex and relationships education, NCB. http://www.ncb.org.uk/media/333301/young_peoples_survey_on_sex___relationships_education.pdf

Sex Education Forum (2011). Survey report: young people’s experiences of HIV and AIDS education. See <http://www.sexeducationforum.org.uk/resources/sex-educational-supplement.aspx>

Sex Education Forum (2013). The Sex Educational Supplement, Issue 1: The Pornography Issue. See <http://www.sexeducationforum.org.uk/resources/sex-educational-supplement.aspx>

UNCRC (2008). 49th session, Consideration of reports submitted by states parties under Article 44 of the Convention, Concluding observations: United Kingdom and Northern Ireland.

UNESCO (2009). International guidelines on sexuality education; an evidence informed approach to effective sex, relationships and HIV/STI education. Paris: UNESCO.

ABOUT THE SEX EDUCATION FORUM

The Sex Education Forum, hosted by the National Children’s Bureau, is the national authority on sex and relationships education (SRE). It is a unique collaboration of national organisations and practitioners with representatives from health, education, faith, disability and children’s organisations. The Sex Education Forum believes that all children and young people have the right to good SRE and aims to provide all professionals involved in SRE with the information they need to ensure this right.

September 2013

Written evidence submitted by Net Children Go Mobile

1. This statement is submitted on behalf of the Net Children Go Mobile Project www.netchildrengomobile.eu by Leslie Haddon and Jane Vincent of the London School of Economics and Political Science, the UK contributors to this EU funded Safer Internet Programme¹⁰⁶ (SI-2012-KEP-411201) led by Giovanna Mascheroni of the Catholic University of Milan.

2. Summary Description of the Structure and Background of the Project:

- The Net Children Go Mobile project is addressing the opportunities and risks for children aged 9–16 regarding their use of mobile internet. In particular it aims to understand and discern the mobile internet experience from the PC-based internet experience.
- The project is delivering comparable findings regarding mobile internet usage, skills, participation and risks among children in UK, Denmark, Italy and Romania.¹⁰⁷
- A quantitative survey of 2000 children has already been completed in these four EU countries. The initial findings on access and use will be reported at the Safer Internet Forum¹⁰⁸ on 17 October 2013, and published on our web site www.netchildrengomobile.eu.
- Data on risks and mediation will be published on the Safer Internet Day, 11 February 2014.
- Qualitative research is currently being conducted and is due for completion in January 2014.
- Topics being explored include:
 - (i) Where and how much children use mobile internet most whilst at home, at school and out and about, and the types of devices they use.

¹⁰⁶ <http://ec.europa.eu/digital-agenda/self-regulation-better-internet-kids>

¹⁰⁷ Additional countries, Ireland and Portugal have now joined this project on a self-funded basis and their results will be included in the analysis during the forthcoming months.

¹⁰⁸ <http://www.cvent.com/events/safer-internet-forum-2013/event-summary-e6c8907d87cf4e719aceb823e13c3463.aspx>

- (ii) Assessment of risk associated with mobile internet compared to accessing the internet generally.
- (iii) Vulnerability factors that indicate which children are particularly risk.
- (iv) Children's awareness of risk and their coping strategies for using mobile internet.
- (v) Parents, teachers and youth/care workers mediation and awareness strategies.
- The research will report on issues including children accessing inappropriate adult content as well as managing abusive and threatening behaviours.
- The outcome will be disseminated in the form of key recommendations relevant to the development of safety awareness and policy.¹⁰⁹

We welcome the opportunity to discuss our findings with the CMS Select Committee both from our UK research as well as the results of the complementary studies by our EU partners from Italy, Denmark, Romania, Ireland and Portugal.

September 2013

Written evidence submitted by British Naturism

INTRODUCTION

As stated by the Committee, the online world poses hazards, ranging from images of child abuse to trolling, that are the converse of the immense benefits of unimpeded communication and free speech provided by the internet, and so any attempt to mitigate harm has to be proportionate and avoid disadvantageous consequences.

British Naturism (BN) is the national organisation that represents naturists in the UK. A full description of Naturism is on BN's website [1] but, in short, *Naturism is the enjoyment of life in every usual way, save that clothes are needed only for physical protection.*

Naturism contains, among other things, a clear *belief* about the universality and acceptability of our one true possession—the human body—and its wholeness.

Our concerns in the debate about Child Safety Online arise when considering topics such as:

- Naturists' use of online methods to maintain and promote naturism.
- Prejudice against minority groups (such as naturists) can drown evidence which supports them.
- Concerns about body image issues in children.
- Safeguarding education in Art, Science, Medical health and Wellbeing, Sex and Relationships.

We deal first with the three issues highlighted by the Committee:

1. PROTECTING MINORS FROM ADULT CONTENT

We agree that minors should be protected from some online content, but qualify this stance as follows:

1.1 Evidence

Any classification of content as “adult” or “inappropriate” must be based on factual evidence, not on emotion, myth or prejudice. The preferences of an ill-informed, perhaps bigoted, minority cannot be allowed to overrule the reasonable attitudes of the majority. For example, some people believe that seeing an image of a naked body is harmful to children, but there is simply no evidence that this is the case. On the contrary, there is much evidence that links prudish attitudes to the body with high levels of eating disorders, body shame and body anxiety in young people.

1.2 Minors

The use of the term “age appropriate” should not be used in legislation without careful definition. Age verification is used, for example, by gambling websites where the possession of a valid credit card forms both the financial security and implicit verification of the person's right to gamble. But in the general case of free access to unsuitable websites, it is unclear to us what mechanism could be devised that verifies the age of the individual who has made initial access, but does not block the unverifiable access by, say, another family member or friend to whom control of the device is passed.

1.3 Filters

Some filters are centrally defined black lists (eg Google SafeSearch), others depend on white lists (eg TwoTen). Our opinion is that white lists are feasible for protecting the youngest children, black lists have drawbacks:

¹⁰⁹ For example some initial findings regarding use of mobile internet in schools have been published <http://www.netchildrengomobile.eu/news/first-findings-of-netchildren-published-on-insafe/>

- They are expensive to research and maintain.
- They cannot ever be completely effective.
- They risk blocking material that is not harmful, and obscuring the fact that blocking is happening.
- It may be very difficult and expensive to challenge unnecessary blocking.

1.4 Regulation

Unlike an industry centred on physical media (films, DVDs, video games) where classification of titles can help the public protect itself from unwanted material, the internet presents a different kind and scale of challenge. By design the internet is constantly growing and changing, so that regulation by any one country is limited to rather crude blocks on major websites (usually those that authorities consider politically destabilising). Satellite mediated mobile telecoms will tend to dissolve national boundaries and render such controls less effective. The suggestion that Ofcom could perform a role like that of the BBFC is clearly infeasible, and the suggestion that Ofcom can set attainable standards for filtering and for age verification is probably not practicable either.

2. FILTERING OUT EXTREME MATERIAL (EG IMAGES OF CHILD ABUSE, AND INFORMATION PROMOTING TERRORISM AND VIOLENCE)

We understand “extreme material” principally to mean content that is already defined as illegal, and we expect that ownership of and access to such content should be prevented by legal means. Organisations such as the Internet Watch Foundation already provide services that identify such dangers, as do investigators in the Police and some charities that have protection in their aims. To the extent that filtering can be made to work, such material should continue to be blocked internationally.

3. PREVENT ABUSIVE AND THREATENING COMMENTS ON SOCIAL MEDIA

We are concerned about the misuse of social media by irresponsible citizens (both adults and children), but think that individual occurrences of such abuse should be identified by those closest to perpetrators and remedial action taken. Legislation already exists to deal with such obviously anti-social behaviour if it persists and causes harm, and both sanctions and education can follow.

Returning to the topics we listed in the Introduction:

4. NATURISTS’ USE OF ONLINE METHODS TO MAINTAIN AND PROMOTE NATURISM

4.1 Blocking

ISPs and MPOs must not be forced or allowed secretly to make inaccessible any website which contains images of the naked human body that are not remotely pornographic.[2] So, for example, the completely legitimate and informative websites that we and other naturists use should never be threatened by over-zealous blocking, especially if there is either no channel for redress or only one entailing expensive litigation.

4.2 Libel

Naturism is a popular, accepted and wholesome lifestyle all over Europe. British naturists should not be forced by legislation into an association with pornography. It would be unacceptable for naturist websites to be subject to filters that may be lifted only by their legitimate users signing up for or opting into a service that, though dubbed “adult”, is considered pornographic by not only service providers but also by other authorities who increasingly try to monitor individuals’ electronic communications. Indeed, such a website and its users could in that circumstance consider that they had been libelled, and initiate legal action.

4.3 Human rights

Freedom of expression protects the interests and images of naturism. There are no restrictions of Art.10 rights due to pressing social need in this context. Indeed, there is a Human Rights ruling which places a positive duty on national governments to protect freedom of expression. The current discussions about legislation give an opportunity to make much more accountable those large corporations that have *de facto* monopolies over some aspects of modern life. The current campaigns to stop Facebook censoring breast feeding illustrate why this is necessary.

5. PREJUDICE AGAINST MINORITY GROUPS (SUCH AS NATURISTS) CAN DROWN EVIDENCE WHICH SUPPORTS THEM

5.1 Largely covered in §1.1 above.

5.2 Blocking or filtering material that not only does no harm to children, but is actually useful or necessary to them, is harmful. Indeed, such blocking would encourage attitudes known to result in widespread and often

serious damage. Additional to §1.1, prudish attitudes also exacerbate body knowledge related indicators such as teenage pregnancy.[3]

6. CONCERNS ABOUT BODY IMAGE ISSUES IN CHILDREN

This subject has seen much discussion in recent years. The overwhelming conclusion is that better education within families and by teachers is needed to mitigate the harmful effects of commercial fashion industry advertising and the concomitant peer pressure experienced by children. BN believes that a proper understanding and acceptance of the human body from an early age provides the best background against which such education can be laid. To risk suppressing this kind of basic information from internet sources would not be helpful.

7. SAFEGUARDING EDUCATION IN ART, SCIENCE, MEDICAL HEALTH AND WELLBEING, SEX AND RELATIONSHIPS

It must be recognised that it is *how* bodies are shown that matters, not *what* is shown. Legislation must take due account of the social and cultural value of material that happens to contain imagery of naked humans. None of the areas listed here is trivial; all may have to refer to the human body as it actually is. Despite the reservations of some minorities, the right to publish and consume such important material is of paramount significance to every new generation in our culture and country.

8. CONCLUSION

In summary, we look to parenting and education to inform children of the risks inherent in internet use, to established authorities to block illegal content, and to society in general to continue to broaden its tolerance of harmless and potentially valuable attitudes.[4]

NOTES

[1] http://www.bn.org.uk/articles.php/_/information/about-naturism/what-is-naturism-r18

[2] Pornography has no universally accepted definition. We take the view that pornography is that sexual material which is in some proven way harmful to society by its influence on adults or children. Thus, accepted sex and health educational material is not pornographic, nor are images of the naked human in Naturalist, Artistic, Scientific and Medical contexts.

[3] We observe, in UNICEF research on teenage birth rates in the rich nations, a clear correlation between high such birth rates and prudish attitudes across the countries studied. The correlation is near perfect, the causal mechanisms well understood, and the effects large. <http://www.unicef-irc.org/publications/pdf/repcard3e.pdf>

[4] This submission is part of a continuing campaign by BN to help keep Naturism, its ideals and its value to society, legitimate and recognised. We would be more than happy to interact with the Select Committee on any of the above issues and opinions or on related ones.

September 2013

Written evidence submitted by the Open Rights Group

We welcome the attention that the Committee is devoting to looking at these important issues and appreciate the opportunity to offer our views.

The areas covered by the Inquiry have been the subject of quite intense, heated and not always helpful or constructive debate this summer. We hope that this Inquiry provides an opportunity for a calm and considered look at these difficult issues.

Open Rights Group have done a significant amount of work on how Internet filtering works over the past few years. That has included:

1. Setting up a website called Blocked.org.uk, which helps us monitor reports of overblocking on mobile phone networks Internet filtering services.
2. In May 2012 producing a report, published jointly with LSE Media Policy Project, looking at how mobile networks implement Internet filtering, in particular addressing issues with overblocking.¹¹⁰
3. A response to the Department for Education consultation on parental Internet controls.¹¹¹
4. In September 2012, co-signing a letter to the Prime Minister alongside a coalition of civil society groups including Index on Censorship, Article 19, Big Brother Watch and Consumer Focus.¹¹²

¹¹⁰ <https://www.openrightsgroup.org/ourwork/reports/mobile-internet-censorship-what-happening-and-what-we-can-do-about-it>

¹¹¹ <https://www.openrightsgroup.org/ourwork/reports/response-to-dfe-consultation-on-parental-controls>

¹¹² <https://www.openrightsgroup.org/ourwork/letters/open-letter-to-the-prime-minister-regarding-parental-internet-controls>

5. A fact sheet summarising some relevant evidence in late 2012.¹¹³
6. Co-signing a joint letter to the Culture Secretary Maria Miller MP in June 2013, along with English PEN, Index on Censorship, and Big Brother Watch, regarding her more recent “summits” with Internet companies.¹¹⁴
7. A list of 20 key questions directed at ISPs regarding their implementation of Internet filtering.¹¹⁵

As an organisation focused on human rights and civil liberties in the digital age, we believe it is possible to reconcile the idea that the Internet can create greater opportunities for exercising the right to freedom of expression with a desire to tackle the problems and dangers young people now face online.

We do not see these as mutually exclusive aims. But we also believe that a simplistic “restrictions” based approach to child safety will: fail on its own terms due largely to the limitations of filtering technology; ignore the wider social issues that young people face; and lead to overly restrictive content practices that reduce the usefulness of the Internet for everybody.

1. HOW BEST TO PROTECT MINORS FROM ACCESSING ADULT CONTENT

In summary, some of our key recommendations to the Government are:

1. Help parents make decisions about what is best for their household.
2. Do not create false expectations about what technology can do, and avoid thinking of filtering and restrictions as the solution.
3. Do not mandate network-level filtering for households. Endorse “active choice”, not default-on, filtering.
4. Distinguish clearly between different types of content and the responses appropriate for each.
5. Acknowledge over- and under-blocking as a serious problem. Ensure that providers of filtering services address this. Ensure they offer transparency regarding what their filters block and why, alongside an efficient, easy to use process for quickly correcting mistakes.
6. Improve sexual health and relationship education and ensure children and young people have supportive and easy to find routes to finding advice and help.

We believe that the Department for Education response to their consultation in December 2012 arrived at a reasonable position—that the Government should help parents make their own decisions about what is best for their household. It has been disappointing to see the Government somewhat turn away from this and effectively mandate default-on filtering.

Challenging the “one click to safety” approach

In his summer speech on filtering and child protection the Prime Minister promised “no more hassle of downloading filters for every device, just one click protection. One click to protect your whole home and to keep your children safe”.¹¹⁶

We believe this is unhelpful and misleading, and runs against the advice of the previous Byron and Bailey reviews of online safety undertaken for the Government.

There is no switch that will keep children and young people safe. If we encourage parents to believe that there is, too many will assume their job is done when they press it. That is to ignore the limitations of the filtering services and the broader issues and pressures that children and young people face online.

Start with good evidence

Too often anecdotes, unsourced figures or insufficiently robust evidence has been used by those in the debate about online safety. We would urge the Committee to base its findings in the best available evidence—and there is plenty of good quality work, for example from the aforementioned EU Kids Online project run by Professor Sonia Livingstone—and also to be rigorous in questioning the evidence presented to it.

Avoiding default-on filters and endorse active choice

There is a risk that default internet filtering will move decisions about what is appropriate for families and households further out of parents’ hands. The Government should instead promote an “active choice” model that encourages parents to make their own decisions about what is appropriate and what tools to use.

We believe the available evidence (for example, from the EU Kids Online project¹¹⁷) does not support an approach focused simply or primarily on filtering restrictions, and certainly not a default “on” Internet filter.

¹¹³ <https://www.openrightsgroup.org/ourwork/reports/parental-controls-and-internet-filtering-fact-sheet>

¹¹⁴ <https://www.openrightsgroup.org/ourwork/letters/culture-sec-content-restrictions>

¹¹⁵ <https://www.openrightsgroup.org/blog/2013/isp-filtering-qs>

¹¹⁶ <https://www.gov.uk/government/speeches/the-internet-and-pornography-prime-minister-calls-for-action>

¹¹⁷ <http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20III/Reports/ParentalMediation.pdf>

Filtering services are error-prone

We know that filtering systems often, through error or overreach, lead to the blocking of legal and legitimate content. This is a byproduct of trying to categorise and filter such a massive volume of content. We would point here, for example, to our work looking at mobile Internet filtering products (which is noted in the introduction). We found amongst others, political blogs, political campaigns, community websites, gay news sites, church groups and technology news sites blocked by accident by mobile networks.

Rather than looking at *whether* this is a problem, policy makers should be asking how to take this fact into account. We are concerned that some vocal supporters of default filtering play down concerns about mistaken blocking, seeing them as just pedantic quibbles.¹¹⁸

There are a number of damaging consequences of ignoring this problem.

First, website owners find it harder to figure out if their site is blocked by one of the filters. This is not an easy task, as most operators of blocking services do not offer an easy way to check URLs (O2 is a notable exception—see their URL checker¹¹⁹). This problem grows when a website owner is faced with a number of blocking services across the various ISPs and service providers, and grows further when they face having to look at other country's policies. If we pretend that over-blocking is not a problem, there will be no effort to improve matters for affected website operators.

Second, our experience of talking to affected website owners is that they find it hard to get their site unblocked when it is mistakenly categorised as “blockable” by a filtering service.

Service providers operating filtering services should be asked how they have assessed the risks of over-blocking and whether they have taken steps to ensure their deployment of filtering tries to address this. They should explain how they will ensure website owners are able to report mistakes and get problems fixed. And service providers should ensure that website owners are able to easily check whether their site has been categorised by the filtering system.

We would like to highlight two damaging consequences of over-blocking—on access to information, and on the economy.

Access to information

First, it would be worrying if sites blocked by accident or through overly broad categories are considered collateral damage of filtering services, as this would be to deny young people access to information at the very moment when it is most important to be helping them satisfy their curiosity and interests.

Filtering can lead to children, young people, and adults being denied access to legitimate and age-appropriate information and resources such as sexual health information and advice.

Filtering that covers different age ranges and/a broadly defined set of “adult” content can deny young people access to material appropriate to their development and needs. In a paper to the EU Kids Online conference in 2011, Tim Davies, Sangeet Bhullar and Terri Dowty argued that filtering can therefore restrict young people's rights in the name of protecting them from risk—specifically “rights to freedom of expression and access to information across frontiers (Article 13, 17), rights to freedom of association (Article 14), rights to preparation for responsible life in a free society (Article 29) and rights to protection of privacy (Article 16)”. They argue that:

“...these broader rights are frequently neglected—with young people's access to information on key topics of health, politics and sexuality limited by Internet filtering—and with a lack of critical formal and informal education supporting young people to gain the skills to live creative and responsible lives in increasingly digitally mediated societies.”¹²⁰

An unintended economic impact

Second, to give a specific example, we heard from the owner of an online gift shop that their site had been blocked by Orange's Safeguard system over Christmas last year. The site sold engraved cigarette lighters, and so we assumed the filters had mistakenly categorised the site under its “tobacco” category. Despite reporting the issue in early December it took until January to get the problem sorted and the site removed from the block list.¹²¹

A larger business may have been able to pressure for a resolution sooner—we see no good reason that smaller businesses should be inhibited in their efforts to reach consumers online in ways larger businesses are not.

¹¹⁸ <https://www.openrightsgroup.org/blog/2013/website-filtering-problems-are-a-load-of-cock>

¹¹⁹ <http://urlchecker.o2.co.uk/urlcheck.aspx>

¹²⁰ See Tim Davies, Sangeet Bhullar, and Terri Dowty, “Rethinking responses to children and young people's online lives”, September 2011, <http://www2.lse.ac.uk/media@lse/research/%20EUKidsOnline/Conference%202011/Davies.pdf>

¹²¹ <https://www.openrightsgroup.org/blog/2013/online-gift-shop-blocked-by-mobile-networks>

To build systems in which less established businesses or organisations are hampered in this way undermines one of the core benefits that the Internet offers for economic and social innovation.

Device based filters are preferable to network level filters

We urge the Committee to look seriously at the relative merits of network-level and device-based filters, across different contexts. We have previously written about some of the benefits and problems of each, and refer the Committee to this previous briefing.¹²²

A healthy market for parental controls is developing; everything proposed regarding filtering technology is available to parents already. Mandating network level filtering would amount to an intervention that could disrupt an emerging market for Internet access tools, whilst imposing significant costs on Internet Service Providers.

The Government's role should be to support this variety of tools and services by working with industry to ensure these are easily available and that parents understand how to use them.

Filtering services block more than pornography

So far the debate has tended to focus on how filters should block "pornography" or even more specifically "hard core pornography". Yet most if not all filtering systems are set up to block a range of categories of content extending beyond adult sexual content. We urge the Committee to look at the variety of content that filtering systems block, how those categories are developed, who considers them to be "18 rated", and what sort of sites those offering filtering think should fall under those categories.

Different categories of material require different approaches

Too often in the recent debate, a variety of different categories of material have been confused and muddled together. That has led to a confused discussion about the appropriate way to deal with such a variety of material.

For example, child abuse images are illegal and dealt with by the Internet Watch Foundation. Other types of unlawful content may be subject to powers that can lead to content being taken down.

Other material that is considered merely unsuitable for people of different ages however—and thus relevant when talking about home Internet filters—will involve more subjective judgments. Those will of course likely vary across households or value systems.

When talking about legal material, there is no easy way to define a category of unsuitable content that young people or children should be protected from. This is especially problematic when considering that filtering can happen in a variety of settings (libraries or shops and cafes or schools or homes or on devices taken across all of them), for a variety of age groups, and for people with a variety of values and beliefs.

We urge the Committee to keep a clear head about the very different types of material at issue and how each requires a different approach when considering how to create safer experiences for young people online across contexts.

Ensuring that policy makers are asking the right questions

We have not been convinced that in pushing the filtering policies forward, policy makers this year have examined the most important practical questions closely enough.

As a result, we have asked 20 questions of ISPs (also noted in the introduction), which cover some of the most significant practical issues with implementation of filtering services including privacy, how choices will be framed and how mistakes will be dealt with. We will submit answers when we receive them. We urge the Committee to look at these questions and consider the extent to which ISPs have addressed them adequately.¹²³

Improve sexual health and relationships education

We support the work of academics such as Professor Andy Phippen, who in his research engages with young people in schools to talk about the pressures and problems they face in a world in which "digital" and "real" life are not distinct.

We support the suggestion that these issues are social problems facilitated by technology that cannot be fixed through technological fixes. We also support the recommendation that we should endeavour to create an environment in which young people feel safe and supported in talking about the problems they face. One aspect of this is to look at improving sexual health and relationship education. So we urge the Committee to look carefully at this context in which children and young people experience problematic material online, rather than just at the limited tools available to try and limit access to some of it.

¹²² <http://www.openrightsgroup.org/assets/files/files/pdfs/Net%20Filtering%20Brief.pdf>

¹²³ <https://www.openrightsgroup.org/blog/2013/isp-filtering-qs>

2. FILTERING OUT EXTREMIST MATERIAL, INCLUDING IMAGES OF CHILD ABUSE AND MATERIAL INTENDED TO PROMOTE TERRORISM OR OTHER ACTS OF VIOLENCE

We would firstly echo our previous comments. For example, as noted above, it is important for policy makers to recognise that we are talking about a variety of different categories of material. We should not assume that it is easy to define what content to filter out for which people or age group, and we should keep illegal and merely objectionable material distinct.

Our comments above about the subjective judgments involved in deciding what content to filter are particularly relevant when looking at a broader range of content. Words like “violent”, “extreme”, “upsetting” or “offensive” will have different meanings to people of different ages, beliefs and will this will vary across different settings.

If policy makers do push for an overly simple approach of specifying broad categories of legal but objectionable content to be filtered in a particular places, it is important to remember that this is not *stopping* these subjective judgement being made. Instead, those judgments are being made by a combination of those in charge of the provision of Internet access in that context (for example, perhaps a building maintenance service), the Internet service providers they use and the filtering service that ISP uses. Each will have their own attitude towards the blockable categories and what material should fall within them. Where these systems are opaque, as they often are, it just becomes harder to understand what decisions about access have been made.

3. PREVENTING ABUSIVE OR THREATENING COMMENTS ON SOCIAL MEDIA

We believe that an important aspect of dealing with this is to create a support system for young people with clear routes for them to report problems and find help.

Once again, it is important to distinguish between different types of behaviour, such as offensiveness, abusiveness or threats, which will require different approaches.

We also urge the Committee to look carefully at the issue of anonymity and relatedly pseudonymity. It is too easy to assume that tackling anonymity online is a simple solution to abusiveness.

In fact, people are usually not truly “anonymous” when they are online. People leave all sorts of information that can identify them. It is sometimes possible to use this information to identify somebody with varying levels of confidence—even if the person posts messages as an “anonymous” or “pseudonymous” user. For example an ISP may try to “match” an IP address with one of their subscribers. There are various legal powers that in some circumstance, require Internet companies to disclose this data, and which permit the use of it in various contexts for the purposes of trying to identify a user.

Further, anonymity in fact serves many positive purposes in a variety of circumstances. For further information, please see our short introduction to anonymity online, available from our website.¹²⁴

September 2013

Written evidence submitted by Russell Pillar

I write in relation to your enquiry into On-line Safety.

This is an issue that has always concerned me and I would like to strongly urge the committee to make a definitive stand for the need to implement greater on-line safety as a matter of urgency.

It is clear that this is a subject that government has been casual about in the past and as a result we now live in a society of young people whose minds are evidently polluted by the despicable material they are able to access on-line.

It is distressing the number of times we read in the newspapers of young persons who have committed suicide after discovering something on-line they didn't know about before, or when they have been bullied on social media. Many times, violent activity is attributed to something a young person has been able to access on the internet.

It is before they reach adulthood that a child's mind is at its most fertile and very easily influenced, therefore perhaps giving us a clue as to why we live in a world where the next generation is becoming more and more extremist in its views due to the vast amount of literature they can access on-line.

I believe this is a trend that we can change if measures are implemented quickly to prevent access of adult material by children under 16 years of age and I would encourage members of the Committee to be bold in their stand and grasp this opportunity to make the world a better and safer place to live in.

September 2013

¹²⁴ <http://www.openrightsgroup.org/assets/files/pdfs/ORG%20anonymity%20introduction.pdf>

Written evidence submitted by CARE

ABOUT CARE

1. CARE is a Christian social policy charity that seeks to combine caring work with public policy research and public policy shaping initiatives. We work in Westminster, Brussels, Strasbourg, Edinburgh, Belfast and Cardiff. We represent approximately 60,000 Christians around the UK, who support our work financially and in other ways. CARE has an interest in helping families protect their children, particularly online. To date our focus has been primarily on trying to ensure that children cannot access age inappropriate content online easily and on helping children deal with online behavioural challenges. This emphasis is reflected in our submission to the Committee.

SUMMARY

2. CARE believes the best way to help parents protect their children online is to have a statutory requirement for companies to provide:

- robust age verification before allowing access to age sensitive content on websites, backed up by financial transaction blocking of such websites that do not comply with the requirement, as introduced by the Gambling Act with respect to online gambling;
- a child friendly internet that would filter at the home network level age inappropriate content from ISPs and Mobile Phone Operators unless and age verified adult “opts-in” to adult content;
- more education for parents coordinated by the secretary of state, conducted by industry; and
- strengthen the powers of Ofcom and ATVOD, including requiring Ofcom to come up with a code of practice.

3. We believe that, in combination, these elements will help parents to parent and thereby help to ensure that children and young people are protected online. We also believe that the proposals are proportionate, and will be welcomed by parents who will be greatly helped by a joined-up safety regime.

THE REMIT OF OUR RESPONSE AND OUR RESPONSE OBJECTIVE

4. Our aim is to put forward the argument that (a) the responsibility to protect children from harmful content is not just that of parents but is wider. (b) Legislative change should be a legitimate option to tackle that problem. (c) There are workable proportionate proposals that would lead to making it harder for children and young people to access age inappropriate content online. The mechanisms will not be perfect but they will be much better than what we currently have. We suggest a battery of mechanisms tailored to empower parents and guardians.

THE PROBLEM

5. Access to streamed hard core pornography or extreme violence which can at times be degrading is very easy for children to stumble upon or access online with no age verification. Moreover, surprisingly large numbers of children are affected. Accessing such content voluntarily or accidentally impacts children’s development.

6. Research commissioned and published in May this year by the Children’s Commissioner concluded with high confidence that:

7. “A significant proportion of children and young people are exposed to or access pornography”.

8. “Children and young people’s exposure and access to pornography occurs both online and offline. However, in recent years **the most common methods** of access have changed from magazines, videos, television and books, with the **internet** becoming more dominant.”

9. “There is some evidence that children and young people consider pornography **easy to access** and culturally prevalent.”

10. “Access and exposure to pornography affect children and young people’s sexual beliefs. For example, pornography has been linked to **unrealistic attitudes about sex; maladaptive attitudes about relationships; more sexually permissive attitudes; greater acceptance of casual sex; beliefs that women are sex objects; more frequent thoughts about sex; sexual uncertainty** (eg the extent to which children and young people are unclear about their sexual beliefs and values); and less progressive gender role attitudes (eg **male dominance and female submission**).”

11. “Children and young people **learn from and may change their behaviour due to exposure and access to pornography.**”

12. “Access and exposure to pornography are linked to children and young people’s engagement in ‘risky behaviours’ (eg engagement in sexual practices from a younger age, engaging in riskier sexual behaviours such as unprotected anal or oral sex, and the involvement of drugs and alcohol in sex). For example, **young people**

who used pornography were more likely to report having had anal sex, sex with multiple partners and using alcohol and drugs during sex.”

13. “Exposure to sexualised material was related to the likelihood of young people engaging in more sexualised behaviour because they perceived more social pressure to have sex.”¹²⁵

14. To compound the general problem described above the increase in fast broadband and mobile connections, smart phones and tablet technology make accessing age inappropriate content more portable and therefore much easier.

15. Parents are said to be given free software and tools that they can use on their families computers. However, the proportion of parents that use such tools is low. The most recent Ofcom study into family media behaviour and parental controls found that:

16. “A smaller number of parents have installed technical controls: 50% of parents of 5–15s have parental controls installed on their multichannel television service; 46% of parents whose child goes online at home have any of the four specific types of online controls asked about installed on their PC, laptop or netbook at home; 31% of parents of 12–15s with a phone that can be used to go online have mobile phone ‘filters’ in place; 14% of parents of 5–15s have parental controls in place on handheld/portable games consoles and 16% on fixed consoles.”¹²⁶

17. While the quantitative statistic show a relatively low uptake of parental controls, Ofcom also commissioned qualitative research into parents view of such controls in order to understand why uptake is low and found that:

18. “After detailed discussion, parents felt that technical parental controls offer the potential for added protection, but that **the available range of controls** is currently **too complex** and **piecemeal**... Parents’ own ‘wish list’ for parental controls also centred on simplicity and included the desire for an easy way to cover all household devices, and to be prompted to install parental controls at the set-up stage or have them preinstalled.”¹²⁷

19. CARE would be the first to say that parental controls cannot be a substitute for other more important parental behaviour such as talking to children about their internet use, setting physical boundaries within the home or how long a computer game can be played. However, we do believe that parental controls are useful in helping and empowering parents to parent their children. Access to unwanted content cannot be helped by other parenting skills, while parents are simply not available 24 hours a day to ensure rules are kept by young people. Finally, the convergence of technology such as smart TVs that allow access to online streamed content, either through game consoles or through newer TVs means that the internet will now be part of television. Parents have said that they want more help and that the tools that help them control the content that their children access online needs to be easier and more user friendly.

THE SOLUTION

20. Since 2009 CARE has worked closely with Baroness Howe of Idlicote, and other concerned parliamentarians, to promote legislative mechanisms that will empower parents to protect their children online and to help children stay safe online. Currently the responsibility falls heavily on parents or guardians, followed by teachers and schools. Our view is that the industry, whether that is website owners, content producers, or internet service providers and mobile phone operators as well as Government could do more to help parents, guardians and teachers protect and educate their children on the safe use of the internet. We don’t mean by this that the industry should intervene to bypass parents to create mechanisms that parent on the parent’s behalf—if indeed such a thing were possible. What we want to see is the empowering of parents with appropriate tools to parent in a technologically new and challenging environment.

21. As the qualitative research commissioned by Ofcom shows, parents want help to ensure they can protect their children. We believe that a cross industry approach with a multidimensional toolbox is the way forward.

SELF-REGULATION SEEMS NOT TO BE ENOUGH

22. Self-regulation has worked in some instances. Most Mobile Phone Operators¹²⁸ and one of the big Internet Service Provider,¹²⁹ have implemented either active choice or opt-in. Here age inappropriate content is filtered unless a person whose age has been verified as 18+ either makes a choice to lift the filter at the beginning of a contract, or opts-in to receiving such content at a later date. It is very clear from the above, however, that whilst there are some models of good practice, these are not the norm and not sufficient.

¹²⁵ All of the above quotes are taken from the report: “Basically... porn is everywhere” A Rapid Evidence Assessment on the Effect that Access and Exposure to Pornography has on Children and Young People, published by the Childrens Commissioner on 23 May 2013 (http://www.childrenscommissioner.gov.uk/content/publications/content_668 accessed 24 September 2013) pp.7–8

¹²⁶ Children and Parents: Media Use and Attitudes Report, Ofcom, October 2012 p.6

¹²⁷ Parents’ views on parental controls Findings of qualitative research, prepared for Ofcom and used in Ofcom

¹²⁸ The code of practice and mobile operators implementations can be found here: http://www.aimelink.org/docs/UK_MNO_Age_Verification_Procedures.pdf (accessed on 25 September 2013)

¹²⁹ Talk Talk have implemented what they call HomeSafe (<http://www.talktalk.co.uk/security/homesafe-demo.html> accessed 25 September 2013)

23. The problem is that not all companies put children's safety at the forefront of decision making. We believe this should be a natural part of business governance, extending to all sites, including those that offer streamed hard-core pornography or violent content. It is true that many adult websites require robust age verification to access 18+ content. However there are many more websites that provide such content for free without robust age verification. Moreover, the business model of these websites can be driven by their click through rate as it relates to advertising. This means that the more clicks a website receives, the more money they make, disincentivising the owners of these websites from applying age verification.

24. When viewed in the round, it is clear that self-regulation is not delivering and that legislative change is required. When considered from an historical perspective this is not so surprising. If one considers the efforts to protect children working in factories during the 19th century, self-regulatory attempts were tried and failed. Only legislative that required everyone to act at the same time worked. Similarly if we jump forward in time to online challenges we find a similar picture. Prior to 2005 parents complained that their children were able to gamble online and were developing gambling problems. The industry responded by making all the right noises. They said that they wanted to do the right thing, that under-age gambling was not in their interest and that they would do their best to prevent such gambling. The necessary change did not happen, though, until the law required everyone to act and every company could be sure that all their competitors would similarly suffer lost revenue and consequently their particular business would be no more disadvantaged than any other. Since the 2005 Gambling Act required online gambling firms operating into the UK to provide robust age verification before players could open accounts on which to gamble there have been no problems with underage gambling at all.¹³⁰

25. Lady Howe has proposed a number of legislative changes to make the online environment significantly safer for children, first, by tabling amendments to Government Bills and, more recently, through her Online Safety Bill.

AMENDMENTS

26. Lady Howe moved amendments to the Digital Economy Bill in which she proposed to make it a requirement for all websites that sold or provided access to what would usually be deemed age sensitive content offline, to have to put into place robust age verification mechanisms before selling or allowing access to such content or products.

27. Enforcement was to have been by imposing: a) ISP blocks on those websites that did not comply with age verification if they were based outside of the UK or b) financial transaction blocking (which tends to be more robust) for such websites.

28. ISP level blocking is used already in the UK to tackle websites that promote copyright infringement. Court orders have forced the largest ISPs to block sites such as 'The Pirate Bay' by using Section 97A of the Copyright, Designs and Patents Act.¹³¹ In this context the failure to back efforts to promote child safety online with legislative action seems very weak. In his NSPCC speech of 22 July, the Prime Minister, addressing child safety online, said 'Nothing is more important than this.'¹³² If that is correct why is it that we are prepared to take robust legal action to protect the copyright, usually of very large multinational companies, but do nothing more than self-regulation when it comes to protecting children online? Moreover, while blocking sites that do not comply with the law is not as effective for people determined to download music or films, it would certainly make it much harder for children to accidentally access streamed hard-core pornography.

29. That being said, we very much welcome The Authority for Television on Demand (ATVOD) move to ask financial services to consider blocking financial services for websites based outside of the UK that stream adult content without having robust age verification mechanisms in place. This is a viable option which we would like to see put on a statutory rather than voluntary footing.¹³³

ONLINE SAFETY BILL

30. Lady Howe has also proposed other mechanisms, which can be found in her Online Safety, private members bill.¹³⁴ This Bill, which is all about empowering parents, makes two key provisions. First, it introduces a statutory opt-in system for both internet service providers and mobile phone operators, to help parents protect their children online.¹³⁵ Second, it introduces new educational assistance (to be provided both by the Secretary of State and the industry) to help parents make best use of the opt-in system for their family

¹³⁰ John Carr the secretary of the childrens charities coalition on internet safety and senior technology consultant to the UN has written on the subject here: http://www.huffingtonpost.co.uk/john-carr/another-step-forward-for_b_1951957.html (accessed 25 September 2013)

¹³¹ <http://www.ispreview.co.uk/index.php/2013/08/uk-government-to-finally-repeal-isp-website-blocking-powers.html> (accessed 25 September 2013)

¹³² <https://www.gov.uk/government/speeches/the-internet-and-pornography-prime-minister-calls-for-action> (accessed 25 September 2013)

¹³³ <http://www.telegraph.co.uk/finance/newsbysector/banksandfinance/10322072/Banks-to-block-internet-porn-sites.html> (accessed 25 September 2013)

¹³⁴ <http://services.parliament.uk/bills/2012-13/online-safety.html> (accessed 25 September 2013)

¹³⁵ There are some parallels with the recommendations made by Claire Perry MP, the Prime Minister's online child safety advisor in an independent parliamentary report, <http://www.claireperry.org.uk/downloads/independent-parliamentary-inquiry-into-online-child-protection.pdf> (accessed 25 September 2013)

and also to help them understand online behavioural challenges (that the opt-in system cannot address) so they can teach their children to stay safe online.

31. It is important to stress that the opt-in system introduced by the Bill does address the problem of false positives, namely when filters block content that should not be blocked. The Bill requires Ofcom to devise codes of standards to be used in filtering. Specifically, Clause 2 (5) states that: "It shall be the duty of OFCOM themselves to establish procedures for the handling and resolution of complaints about the observance of standards set under this section." This would include a mechanism for the timely resolution of any complaint made by an owner of a website that should not be filtered.

FLAWED ARGUMENTS AGAINST STATUTORY OPT-IN

32. One argument that is used against statutory opt-in is that it is censorious. This is obviously not the case. Adults can access whatever content they like and our society has long held that there is content that children should not have access to, which is why we have the watershed on TV, and licensed sex shops to sell 18+ content.

33. Another argument pertains to the efficacy of blocking. To suggest that because no opt-in system will be 100% foolproof, it is a failure is to completely misunderstand the purpose of opt-in. Although there are ways to try and get around the protections provided by opt-in, one must not forget the following:

34. First, not all children and young people will want to seek out adult content but will stumble across it. This would not happen with easy home network level filters. Second, even if a child or young person does want to seek out adult content and finds out how to get around the filters through trying to setup a proxy, filters can be set to block websites that offer free or paid for proxy services. Many office networks are set in such a way. Why should this not be the case on a home network? Third, VPN services usually cost money. While the most dedicated teen might be able to get their hands on a payment system and setup a VPN connection, their ingenuity and tenacity might be something we should silently applauded, while also remembering that these cases will not be the majority.

35. Here we need to remember that no law is perfect and perfectly upheld. This proposal would not be perfect either, however it would be a marked, proportionate improvement on our current situation.

IN CONCLUSION

36. CARE believes the best way to help parents protect their children online is to have a statutory requirement for companies to provide:

- robust age verification before allowing access to age sensitive content on websites, backed up by financial transaction blocking of such websites that do not comply with the requirement, as introduced by the Gambling Act with respect to online gambling;
- a child friendly internet that would filter at the home network level age inappropriate content from ISPs and Mobile Phone Operators unless and age verified adult "opts-in" to adult content;
- more education for parents coordinated by the Secretary of State, conducted by industry; and
- strengthen the powers of Ofcom and ATVOD, including requiring Ofcom to come up with a code of practice.

37. We believe that in combination these elements will ensure that children and young people are protected much more than they have been, that the proposals are proportionate, and that they will be welcomed by parents who will be greatly helped by a joined-up safety regime.

September 2013

Written evidence submitted by Malcolm Holmes

I present the following submission to the Committee as having a serious concern regarding the mind bending powerful influence of the media and internet. Young people have very receptive minds capable of remembering sights and images which can become seared into their thought processes.

As a Christian and acutely aware of the decline in moral standards in the western world, the uncontrolled access to pornography, and the ease with which online grooming and sexting, on the part of unscrupulous men in particular, can access vulnerable young people is alarming to say the least. The need of control of the corrupting content of adult content being accessed by youthful fertile minds is long overdue.

The technology for default blocking and use of filtering, to control and filter out unsuitable adult web pages is already available given the will to use it, there is no reason this cannot be made a mandatory requirement.

I appeal to the Committee to use their influence to ensure that an adequate provision is made for safety measure to be implemented.

September 2013

Written evidence submitted by Microsoft UK

Microsoft welcomes the opportunity to respond to the Culture, Media and Sport Select Committee's Inquiry into Online Safety. It is right that these important issues are given a high priority and Microsoft is grateful for the opportunity to share with the Committee the work we are doing in this area.

HOW BEST TO PROTECT MINORS FROM ACCESSING ADULT CONTENT

1. Windows Vista, Windows 7 and our latest release Windows 8 all include parental control features to help parents monitor, manage, and administer their children's computer use and help keep them safe. The Family Safety Center in Windows 8 gives parents two ways to limit the internet content their child is allowed to view. They can use web filtering to set broad categories of sites that their child can visit. For example, they might allow them to see known child-friendly and general-interest websites, while automatically blocking any sites that provide adult content. They can also allow or block individual websites by their web addresses or URL. When a parent turns on Family Safety for a child's user account, monitoring starts automatically. They will then receive regular activity report emails from Family Safety, showing how much time their children spend on the computer, the websites they visit, the games and apps they use, and the terms they look up on search engines like Bing.

2. Microsoft also offers parents the opportunity to set limits on Bing by keeping sites that contain sexually explicit content out of search results using the SafeSearch settings of strict, moderate or off. When web filtering is enabled, SafeSearch is locked to strict for popular search engines like Bing, so links to adult content including images and videos are not shown and advertising for adult sites is also not shown.

3. The Xbox 360 console lets users customise and manage their family's access to games, films and television content. The Xbox 360 parental controls can be used to control the console itself and access to Xbox Live. Parental controls allow users to control things such as which games can be played, which films and TV shows can be watched and how long each family member can use the console on a daily or weekly basis. Parents can also change the online safety and privacy settings for the account or a managed dependent account to block or allow access to Internet Explorer for Xbox, determine who can see their profile and for parents, determine if approval is required to accept or send friend requests.

4. Education is key in the protection of children and for many years we have been focused on educating both children and parents around these issues. Microsoft has an extensive safety and security site which can be found at www.microsoft.com/safety and we have produced a number of useful documents, such as:

- Is your teen a good Digital Citizen?
- Teach kids mobile safety.
- Protecting young children online.
- Protecting "tweens" and teens online.
- Help kids stand up to online bullying.

5. In the UK we have worked with the Education arm of CEOP for the last five years. Over 200 of our UK employees are trained to deliver CEOP's ThinkUKnow resources in school, and we also give presentations to parents. More recently we have supported The ParentZone in producing a new resource for practitioners to be able to educate parents more effectively around internet use. "Parenting in the Digital Age" is a one day course that trains teachers and others to be able to better advise parents, giving them the knowledge and confidence they need to find out what their children are doing online, where they go and who they talk to. We also have a strong relationship with the UK Safer Internet Centre and we have hosted Safer Internet Day activities for them at our London offices each year for the last three years.

FILTERING OUT EXTREMIST MATERIAL, INCLUDING IMAGES OF CHILD ABUSE AND MATERIAL INTENDED TO PROMOTE TERRORISM OR OTHER ACTS OF VIOLENCE

6. Microsoft is committed to removing access to child sexual abuse content within our Bing search results globally and we undertake proactive efforts to detect, flag and remove child sexual abuse content in addition to responding to third party requests.

7. Microsoft is a member of the Internet Watch Foundation (IWF) and we work closely with them to fight child sexual abuse. We also respond to reports made by users or law enforcement agencies across all our markets worldwide. To avoid bad actors becoming aware of (and bypassing) our systems to minimise child sexual abuse content in our search results, we will not describe our efforts in detail here.

8. Microsoft has also developed PhotoDNA, a technology that aids in finding and removing child abuse images from the internet. PhotoDNA is an image-matching technology which creates a unique signature for a

digital image, like a fingerprint, which can be compared with the signatures of other images to find copies of that image. The IWF, the National Center for Missing and Exploited Children (NCMEC) in the US and online service providers already use PhotoDNA to help find, report and eliminate child abuse images online.

9. Many online service providers have worked with NCMEC and Microsoft to help stop the redistribution of the worst images of child abuse material known to NCMEC. However, early on in the PhotoDNA effort, Microsoft also heard very strong interest from law enforcement for the potential to use the technology to assist in their own investigative efforts—in particular as a means to help them analyse the large number of child abuse images in their own databases, identify correlations between cases and, perhaps most importantly, swiftly identify whether an image is new to them and there may be an active abusive situation with a new victim. Microsoft worked with law enforcement to determine the best ways to apply PhotoDNA to address that need and, in March 2013, we announced that we were making PhotoDNA available to law enforcement at no charge via a number of channels including NetClean Analyze (a free technology already used by law enforcement in many countries worldwide), the Child Exploitation Tracking System (CETS) and direct licensing. CETS is a collaborative global law enforcement programme which helps law enforcement agencies (including CEOP) to follow hundreds of suspects at a time and eliminate duplication, making it more efficient for the agencies to follow up on leads, collect evidence and build cases against suspected child abusers. More information about all of these efforts can be found at <http://www.microsoftphotodna.com>.

10. Regarding terrorist and extremist material, it is important to distinguish between content on the internet which is illegal because it stirs up hatred on the grounds of race, religion or sexual orientation, and content which may be extremist and offensive but is legal. When Microsoft receives a notice from UK law enforcement of a URL that contains verifiable evidence of illegal hate content we will expeditiously remove it from the Bing UK search results.

11. We have had a number of conversations with the Office for Security and Counter-Terrorism, in the Home Office around the Prevent strategy which is looking at how the internet industry and Government can work together regarding unlawful terrorist related materials online and we are working with them to help them understand our search technology.

12. Advertising on Bing UK that facilitates or promotes hate speech is not allowed, whether directed at an individual or a group. This includes any content intended to degrade, intimidate, or incite violence or prejudicial action against a group of people based on their race, gender, ethnicity, national origin, religion, sexual orientation, disability, or other differentiating factors. All adverts are filtered against a list of keywords in well-known phrases containing hate speech. As with copyright content, Microsoft operates a notice and takedown policy for advertising which facilitates and promotes terrorist and extremist material and editorial staff will remove it immediately if they receive a complaint that it violates our policy.

13. Following the Prime Minister's speech on online safety in July, we are in discussions with the Government about the further action the industry can take to tackle online child abuse content. However, as the talks are ongoing, we can not share any further information at this time.

October 2013

Written evidence submitted by The Authority for Television on Demand

EXECUTIVE SUMMARY

E.1 This submission is from The Authority for Television On Demand ("ATVOD"), the independent co-regulator for the editorial content of UK video on demand services. Of particular relevance to this inquiry is our experience of regulating UK based websites which offer pornographic video content on-demand. This submission therefore concentrates on how best to protect minors from accessing adult content.

E.2 ATVOD welcomes the inquiry. Although regulation can do much to protect minors from adult content, ATVOD considers that current regulatory rules and voluntary initiatives do not sufficiently address the challenges of protecting children in a converging media world, especially in relation to the widespread availability of free hardcore pornography which can be accessed by under 18s.

E.3 ATVOD supports recent initiatives to increase the uptake of parental control software, but considers that further action will also be required if children are to be adequately protected.

E.4 In the first part of this submission, ATVOD briefly sets out:

- The action ATVOD takes to ensure that minors cannot access adult material when using UK based video on demand services (including pornographic services).
- The extent to which the provision of pornography online is dominated by services being provided from outside the UK (but accessible from within the UK), such services being beyond ATVOD's remit.

E.5 In the second part of this submission we invite the Committee to consider three main areas and pose questions in relation to each:

- The legal framework for the regulation of UK video on demand services, including:

- Should greater certainty be provided in relation to the statutory basis for requiring hardcore pornographic material on UK based video on demand services to be kept out of reach of children?
- Is it appropriate that content which is prohibited for sale to adults on a DVD, even in a licensed sex shop, can be made available to adults on a UK video on demand service?
- Is it too easy for those who operate pornographic websites to conceal their identity?
- The existing criminal law:
 - Is the Obscene Publications Act being used to best effect?
- Other public policy measures, especially in relation to non-UK services:
 - Can media education be the whole solution?
 - Can the uptake and efficacy of parental control software be improved?
 - Can a consensus for action be built among EU Member states?
 - Should non-EU VOD services which are targeted at the UK be brought within the scope of regulations designed to protect UK consumers and children?
 - Should UK financial institutions refrain from processing payments to non-EU services operating in breach of the Obscene Publications Act?

I. INTRODUCTION

1.1 The Authority for Television On Demand (“ATVOD”) was designated by Ofcom in March 2010 to regulate the editorial content of UK video on demand services. Its duties and powers derive from the EU Audiovisual Media Services Directive (“AVMSD”) which was implemented in the UK via amendments to section 368 of the Communications Act 2003 (“the Act”). Under the Act, UK services which meet the statutory definition of an on demand programme service (“ODPS”) must comply with a limited number of statutory requirements which have been incorporated by ATVOD in a set of Rules. To meet the definition of an ODPS a service must meet all five of the criteria set out in section 368A of the Act. Among these are the criteria that a service must have the principal purpose of providing “tv-like” programmes and that the provider of the service must be under UK jurisdiction.

1.2 ATVOD’s primary role in relation to protection of minors is founded in Article 12 of the AVMSD, which forms ATVOD’s Rule 11:

“Rule 11: Harmful Material: Protection of Under-18s

If an on-demand programme service contains material which might seriously impair the physical, mental or moral development of persons under the age of eighteen, the material must be made available in a manner which secures that such persons will not normally see or hear it.”

1.3 ATVOD’s interpretation of this Rule is that “material which might seriously impair the physical, mental or moral development of minors” when provided as part of an on-demand programme service may include content that has been classified “R18” by the BBFC, or material equivalent to content classified in that category. R18 is the UK film and DVD classification for audiovisual works which (a) have the primary purpose of sexual stimulation and (b) include explicit images of real sexual activity or strong fetish activity. Such material is referred to as “hardcore porn” in this submission. To comply with ATVOD Rule 11, an ODPS offering hardcore porn must ensure that such images are kept out of reach of children by having in place a robust age verification mechanism and a means of restricting access to hardcore porn material to those whose age is known to be at least 18. ATVOD considers that the following will normally be considered suitable mechanisms for verifying age:

- Confirmation of credit card¹³⁶ ownership or other form of payment where mandatory proof that the holder is 18 or over is required prior to issue.
- A reputable personal digital identity management service which uses checks on an independent and reliable database, such as the electoral roll.
- Other comparable proof of account ownership which effectively verifies age.

If age verification does not take place each time the user returns to the service, the service provider must control further access to hardcore porn material by the use of mandatory security controls such as passwords or PIN numbers. ATVOD’s full guidance on Rule 11 (and on the other 12 rules it enforces) is published in its Rules and Guidance.¹³⁷

1.4 In addition to investigating complaints, in 2012–13 ATVOD carried out a number of targeted investigations and such investigations resulted in 18 cases¹³⁸ across 26 websites in which breaches of Rule 11

¹³⁶ ATVOD does not regard confirmation of ownership of a Debit, Solo or Electron card or any other card where the card holder is not required to be 18 or over to be verification that a user of a service is aged 18 or over

¹³⁷ http://www.atvod.co.uk/uploads/files/ATVOD_Rules_and_Guidance_Ed_2.0_May_2012.pdf

¹³⁸ Details of these determinations are published at <http://www.atvod.co.uk/complaints/complaint-determinations>

were determined because the services were making available “hardcore” pornographic material without having adequate safeguards in place to ensure that such material could not normally be seen by under 18s.¹³⁹

1.5 In 15 cases the breaches were brought to an end shortly after the Determination that a breach had occurred, though in two of these cases ATVOD had to use its power to issue an Enforcement Notification in order to secure compliance. In the other three cases, the matter was referred to Ofcom for consideration of a sanction. Ofcom imposed the following financial penalties in relation to those cases:

- Playboy TV (provided by Playboy TV UK/Benelux Ltd): £35,000.
- Demand Adult (provided by Playboy TV UK/Benelux Ltd): £65,000.
- Strictly Broadband (provided by Strictly Broadband Ltd): £60,000.

1.6 The Demand Adult and Playboy TV services are no longer being provided by Playboy TV UK/Benelux Ltd (a company registered in the UK, and subject to ATVOD regulation) after a group re-organisation by a parent company which operates across multiple jurisdictions. The Strictly Broadband service was sold to a provider outside the UK following the ATVOD Determination. ATVOD has no evidence that such changes were made in order to place the services outside UK jurisdiction in order to avoid the need to put in place age verification and access control mechanisms which would ensure that explicit content is kept out of reach of under 18s, but that is the effect. ATVOD has also seen a number of examples in which it is claimed that editorial responsibility for a service has been transferred from a UK provider to an entity outside the UK, for example through the sale of the website, while the UK entity continues to supply content to the service. Although ATVOD requires evidence that any such transfer of editorial responsibility is genuine, it is clear that moving is an option for a service which seeks to avoid the obligations placed on UK providers.

1.7 Given the response of a minority of providers of adult services to enforcement of Rule 11, ATVOD has considered how children might better be protected from hardcore pornography online, and especially from such material on websites operated from outside UK jurisdiction, whether from other EU Member States or from outside the EU altogether.

1.8 ATVOD is acutely aware that the hardcore porn services most commonly accessed from within the UK are operated from outside the UK. The most frequently accessed services¹⁴⁰ use a variation on the You Tube business model (and are consequently commonly referred to as “tube sites”). Such tube sites offer significant quantities of unrestricted free hardcore porn videos as a shop window in order to attract large number of viewers whose visits are monetised in a number of ways: by up-selling to a premium version of the free service (offering a wider choice, longer videos, better picture quality, etc); by driving traffic to other paid (pornographic) services operated by the provider of the tube site; by charging on a “click through” basis to affiliates whose content is featured on a “try before you buy” basis on the tube site; and by selling advertising space (eg for “contact” services or penis enlargement treatments).

1.9 Even those non-UK hardcore porn services which operate a more traditional business model, requiring payment before the user can access significant quantities of video material, typically offer free access to hardcore still images and “preview” videos on an unrestricted basis.

1.10 As noted above, provided the services are operated by entities outside UK jurisdiction they are not subject to regulation in the UK, even if the service appears to be specifically targeting UK users or otherwise has a strong association with the UK. Options for addressing this issue—such as blocking payments to services which allow minors to access hardcore porn—are discussed in section two.

1.11 A significant minority of such services operate from other EU Member States. Such services are subject to the same AVMS Directive requirements as UK based services, however not all EU Member States share ATVOD’s view that hardcore porn might seriously impair the development of under 18s. For example, in the Netherlands, the regulator takes the view that hardcore porn does not seriously impair the development of under 18s and so hardcore porn services operating from the Netherlands are not required to ensure that under 18s cannot normally see or hear the hardcore porn material. The AVMS Directive includes derogation procedures¹⁴¹ which might allow the UK to restrict services operating from another Member State on the grounds that such restriction was necessary to protect minors, however such measures would be subject to the examination of the Commission who would ask the UK to refrain if the measures were considered incompatible with European Union law. ATVOD notes that to date UK Govt has not used the derogation procedures in relation to on-demand media services regulated in other Member States.

1.12 Even if the problem was solved at a European level, the majority of online hardcore porn services which allow UK children to see hardcore porn material, and which are most commonly accessed from the UK, operate from outside the EU (most commonly from the USA). As well as the standard website version of the service, the content is commonly provided in a parallel web-version formatted specifically for access via a smartphone.

¹³⁹ Such investigations have continued during 2013–14 and have resulted in a further 11 services being found in breach of Rule 11 as at 30/09/13.

¹⁴⁰ Pornhub, xHamster, XNXX, RedTube, Xvideos, YouPorn, Tube 8 (as measured by Alexa Rankings, see footnote 142 below)

¹⁴¹ Article 3 para 4

1.13 An indication of the scale of the problem can be gained from web analytic data which suggests that five of the top 50 websites most commonly accessed from the UK are tube sites offering unrestricted access to hardcore porn videos.¹⁴² ATVOD has seen figures which suggest that those five hardcore porn tube sites were (collectively) visited over 214 million times by UK internet users during January 2013.

1.14 Although accurate figures for children accessing hardcore porn online are difficult to find, it is worth noting that, according to Ofcom research:¹⁴³

- 62% of 12–15 years old have a smartphone.
- 12–15 year old on average spend 17.1 hours a week online.
- 43% of 12–15 year olds mostly use the internet in their bedroom.
- 55% of 12–15 years mostly use the internet while alone.

1.15 Although the problem has existed for some years it has recently become much more visible and has acquired much greater potency over the past year. This is evident in the results of research¹⁴⁴ conducted by ICM Research on behalf of ATVOD which found that:

- 77% of British adults think hardcore porn videos are easy for children to see online.
- 88% of British adults think it is important that UK websites offering porn-on-demand are required to take the steps set out in the ATVOD Rules and Guidance—such as restricting access, to credit card holders or by checking information against a reliable database, eg the electoral roll—to ensure that under 18s do not normally see hardcore porn material.
- Women are particularly concerned, with 94% saying the measures required by ATVOD are very or quite important (with 82% specifically saying they are very important).
- Overall, 69% of British adults say the measures required by ATVOD are “very important”.
- Views are broadly the same for adults with or without children.

1.16 The transformation of the business of monetizing hardcore porn material online over the past 10 years, and the technological changes that enable minors to have unsupervised access to the internet can only have increased the likelihood of minors accessing explicit adult material online, despite the effective interventions undertaken by ATVOD in relation to UK based porn on-demand websites.

2. IMPROVING ONLINE SAFETY

2.1 This section sets out questions that the Committee may care to take into account when considering how best to protect children from the hardcore pornographic material which is available online.

The legal framework for the regulation of UK video on demand services

Should greater certainty be provided in relation to the statutory basis for requiring hardcore pornographic material on UK based video on demand services to be kept out of reach of children?

2.2 Under Part 4A of the Communications Act 2003 (“the Act”), ATVOD requires UK providers of pornographic on-demand services which meet the statutory definition of an on-demand programme service (“ODPS”)¹⁴⁵ to ensure that any hardcore pornographic material on their service is normally kept out of reach of children. ATVOD’s policy derives from its view that hardcore porn, equivalent to that passed R18 by the BBFC, *might* seriously impair the moral development of minors and a precautionary approach is therefore appropriate.

2.3 At the request of DCMS, in 2010 Ofcom produced a report¹⁴⁶ which indicated that there was uncertainty as to whether R18-equivalent material “*might seriously impair*” under 18’s. In its 2011 response,¹⁴⁷ Government stated that it intended to address this issue comprehensively in the ongoing Communications Review of the current regulatory framework. Government also supported the ATVOD position in stating that there was a good case that the existing Regulations require a precautionary approach. Ofcom and ATVOD were asked to take any steps necessary in the interim period to ensure that children remain adequately protected under the ATVOD Rules, in the knowledge that Government could bring forward further Regulations in the short term if it proved necessary to support this position. Adopting the precautionary principle, ATVOD had already concluded that R18 equivalent material might seriously impair the development of under 18s, and ATVOD continues to interpret the legislation in that way (see paras 1.2 to 1.5 above).

2.4 The DCMS strategy paper (“Connectivity, Content and Consumers”) published in July 2013 sets out Government’s intention to legislate to make clear that R18-equivalent material on ODPS must be provided

¹⁴² Source: Alexa Rankings for 05/07/13—rank is calculated using a combination of the estimated average daily unique visitors to the site and the estimated number of page views on the site over the past three months

¹⁴³ Ofcom—Children and Parents: Media Use and Attitudes Report, 23 October 2012

¹⁴⁴ Online study, conducted by ICM Research on 26–27 September 2012, and involving responses from a demographically based sample of 2019 adults in Great Britain. Full report at <http://www.atvod.co.uk/news-consultations/news-consultationsnews/20121203-porn-and-hatred-online>

¹⁴⁵ as defined in section 368A(1) of the Act

¹⁴⁶ <http://stakeholders.ofcom.org.uk/internet/Sexually-Explicit-Material-VOD.pdf>

¹⁴⁷ <http://www.culture.gov.uk/images/publications/EVletter-to-ed-richards-3aug2011pdf.pdf>

only in a manner which ensures that under 18s do not normally see or hear it. ATVOD considers that such legislation would provide clarity for consumers and industry and better ensure deployment of effective safeguards. Such legislation would also remove the possibility of ATVOD's consumer protection measures being undermined by a legal challenge. The Committee may therefore care to consider whether to support the proposed legislation, and what form it might take.

*Is it appropriate that content which is prohibited for sale to adults on a DVD, even in a licensed sex shop, can be made available to adults on a UK video on demand service?*¹⁴⁸

2.5 Some video on demand services contain hardcore pornographic material which goes beyond the limits of R18. This means that on a DVD it would not be classified by the BBFC for supply to adults in a licensed sex shop. Currently, the Act does not prohibit such content on an ODPS provided it is restricted to adults. Consequently, material which is considered to carry such a risk of harm that it cannot lawfully be supplied on a DVD to adults who visit a licensed shop is freely available to adults on video on demand services which operate and are regulated in the UK. Although ATVOD's interpretation of the statutory requirements mean that UK video on demand services must prevent minors accessing such content, its availability to adults nevertheless poses a potential risk to children. This is because material which goes beyond the limits of R18 may include pornography which simulates non-consensual sex, under-age sex, incest or other material likely to encourage an interest in abusive sexual activity which, through its impact on adult viewers, may ultimately have a detrimental effect on minors.

2.6 The Communications Act 2003 only prohibits on ODPS material which is likely to incite hatred. Pornographic content would not ordinarily fall into this prohibition.

2.7 The DCMS strategy paper ("Connectivity, Content and Consumers") published in July 2013 sets out Government's intention to legislate to prohibit on an ODPS material which is "beyond R18". The Committee may therefore care to consider whether to support the proposed legislation, and what form it might take.

Is it too easy for those who operate pornographic websites to conceal their identity?

2.8 Determining whether a service is an ODPS and who is the provider is central to ATVOD's regulatory remit. ATVOD proactively investigates whether pornographic services which appear to be provided from the UK meet the relevant statutory criteria and therefore fall within the scope of the regulations it enforces. Often the decision turns on whether the provider of the service (ie the person who exercises general control over the selection and organisation of the programmes) is within UK jurisdiction. Providers of pornographic services frequently neglect to publish contact details or even the name of the provider. Without this information it is impossible for ATVOD to determine that the service is an ODPS.

2.9 To enable such investigations, the Act confers upon the regulator a power to demand information from "a person who appears to them to be or to have been a provider of an on-demand programme service".¹⁴⁹ While this power is useful where a service can be linked to a person¹⁵⁰ who appears to be the provider (eg because the website is registered in their name, or because they are listed on the service as holding proof of age records for the performers), in many cases the only identifiable person is the third party payment processor. Current legislation does not appear to give the regulator power to demand information (such as the identity and contact details of the recipient of the payments) from an entity such as a payment processor which is clearly not itself the service provider.

2.10 The Committee may therefore care to consider whether it is currently too easy for UK providers of porn on demand to hide behind third party payment processors, proxy registration services¹⁵¹ and other third parties which provide support services or content to the service. One way in which the current UK regulatory arrangements might be made more effective without extending the scope of content regulation would therefore be to include provisions relating to those who provide financial, hosting or proxy registration services which facilitate the provision of an ODPS in a manner which obscures the identity of the service provider. Such ancillary services could then be required to provide to the appropriate regulatory authority information necessary to identify the provider of an ODPS.

The existing criminal law

Is the present law—notably the Obscene Publications Act 1959 & 1964 being used to best effect?

2.11 In carrying out its statutory regulatory duties, ATVOD has drawn attention to the current Crown Prosecution Service ("CPS") guidance for prosecutors on the interpretation of the Obscene Publications Act ("OPA"), which states that:

¹⁴⁸ This refers to material which would not be classified even at R18 by the BBFC. Currently the law only requires that such material is limited to on-demand viewers who are over 18, even though it would be unlawful to supply the material to adults on a DVD, even in a licensed sex shop.

¹⁴⁹ Section 368O of the Act

¹⁵⁰ A company is a 'person' for these purposes

¹⁵¹ Such services register a web domain on a behalf of a third party in order to preserve the anonymity of that third party

“where children are likely to access material of a degree of sexual explicitness equivalent to what is available to those aged 18 and above in a licensed sex shop, that material may be considered to be obscene and subject to prosecution. This applies to material which is not behind a suitable payment barrier or other accepted means of age verification, for example, material on the front page of pornography websites and non-commercial, user-generated material which is likely to be accessed by children and meets the threshold. see R v Perrin, [2002] EWCA Crim 747.”

Yet ATVOD can find no recent example of a prosecution being launched under that guidance. This seems all the more remarkable in the light of research findings showing the extent of consumer/parental concerns.¹⁵²

2.12 The Committee might therefore question why prosecutions under the OPA in relation to online content in recent years appear to have been limited to websites offering material which is more extreme than would be available in a licensed sex shop. Furthermore, such OPA convictions have declined dramatically in recent years, from 81 in 2000 to just seven in 2010.

2.13 Given the disparity between the CPS guidance and actual enforcement activity under the OPA, might this be an area to explore in order to strengthen the protections for children online? Significant enhancement of consumer protection could be achieved through operational change by the police, without the need for further legislation or public policy revision.

2.14 ATVOD also notes that the provisions of the OPA allow a conspiracy charge to be brought against a person responsible for distributing, retailing or producing the obscene material. Might this enable action to be taken against UK entities or persons who are involved in the provision of hardcore porn without suitable controls, but who do not meet the narrow definition of an “ODPS service provider”?

Other public policy measures, especially in relation to non-UK services

Can media education be the whole solution?

2.15 There is widespread support for initiatives designed to inform and empower parents about the risks children face on line and the steps they can take to protect them. ATVOD also actively supports such initiatives, not least through its work with UKCCIS on age verification tools and “active choice” initiatives for internet connected TVs, and through its support for Safer Internet Day. However, given its limitations, not least with regard to the most vulnerable children, can media education alone ever be sufficient if children are to enjoy appropriate protection from exposure to hardcore pornography online?

Can the uptake and efficacy of parental control software be improved?

2.16 ATVOD supports initiatives to improve the take up of parental controls, not least because it is aware that the use of filtering software by parents is significantly lower than might be desired, and has not been rising. It is not clear why more than six out of 10 households with child internet users do not use parental control software, but as such software is often pre-installed or available free as part of a contract with an ISP, it is unlikely that cost is a significant factor. Research¹⁵³ has indicated that parents who are regular and confident internet users, who say they worry a lot about their children seeing inappropriate material online, and who have younger children, are more likely to use parental control software. Yet there remains a lack of clarity about the reasons why so many parents do not. The impact of recently announced policy changes designed to build upon the active choice initiative will need to be carefully monitored.

2.17 The usefulness of parental control software depends not only on its uptake but also on its effectiveness. This is especially important lest parents who use parental control software are lulled into a false sense of security about the extent to which their children have been protected when using the internet. Should the public debate around parental controls therefore also concentrate on improving understanding of the limitations of parental controls software, especially in terms of efficacy in blocking inappropriate content on protected devices or networks?

2.18 ATVOD notes that five years after the Byron Report recommended a BSI Kitemark for such software only one product¹⁵⁴ carries the relevant Kitemark. ATVOD further notes that EU Commission research¹⁵⁵ suggests that the filters themselves when set to block “adult” content suffer from relatively high rates of over-blocking (accidentally blocking non-adult sites) and under-blocking (failure to block adult sites). The under-blocking rate varies greatly, from 9% to 54% and those with lower under-blocking rates tend to have higher over-blocking rates. Some of the best known filtering options had significant failure rates. For example:

- MacAfee Internet Security was found to under-block 50% of the time, and over-block 27% of the time;

¹⁵² See, for example, research conducted by ICM Research for ATVOD (<http://www.atvod.co.uk/news-consultations/news-consultationsnews/20121203-porn-and-hatred-online>)

¹⁵³ Livingstone, S, Ólafsson, K, O'Neill, B, and Donoso, V (2012). *Towards a better internet for children: findings and recommendations from EU Kids Online for the CEO Coalition*. LSE, London: EU Kids Online. <http://eprints.lse.ac.uk/44213/>

¹⁵⁴ Netintelligence, PAS74 Internet Safety—Access Control Systems for the protection of children on line

¹⁵⁵ Source: Benchmarking of parental control tools for the online protection of children SIP-Bench II—EU Safer Internet Programme (2011). Table 10, page 26

- Net Nanny was found to under-block 41% of the time, and over-block 1% of the time;
- Windows Live Family Security was found to under-block 9% of the time, and over-block 54% of the time

Overall, the study concluded that “In general, [PC parental control] tools have a low effectiveness.”¹⁵⁶

2.19 Although the efficacy of parental controls may have improved since that research was conducted in 2011, it is clear that both “over-blocking” and “under-blocking” still occur. Both must be of concern. Under-blocking because it allows children to access material which is supposed to be blocked, and over-blocking because by restricting access to legitimate content it undermines confidence in the software. ATVOD also notes that parents are much more likely to have anti-virus software enabled than to have parental controls enabled (67% compared with 39% according to Ofcom research¹⁵⁷). Some of this differential may result from parents disabling a parental control system when it is found to over-block.

2.20 The Committee may therefore care to consider whether public policy initiatives to improve take up of parental controls in households with children should be balanced by efforts to improve the efficacy of the systems available to parents. If so, it may be sensible to keep in mind the fact that if all responsibility is placed on parents, many children will remain unprotected.

Can a consensus be built among EU Member states?

2.21 The UK is joined by at least five other EU states¹⁵⁸ in requiring services that provide access to hardcore pornographic material to ensure that such material is kept out of reach of children. However, many other EU states impose no such restrictions, and service providers operating from within The Netherlands, for example, do target the UK consumers with hardcore pornographic video on demand websites which offer inadequate (or non-existent) protections against access by children. ATVOD has no power to insist on such protections being offered by these services.

2.22 Providers established in Member States which do not require such restrictions on VOD pornography services would argue against any attempt at extra-territorial criminal arrest and prosecution by the UK (eg under the OPA by means of a European Arrest Warrant.) They would say such action would infringe their right to freely provide services in the EU under the country of origin principle enshrined in the AVMS Directive (Article 3). To take action, the UK would therefore have to derogate on the grounds that the measures are necessary for reasons of public policy (eg the protection of minors) or for the protection of public health, and would be required to notify the Commission. Any such action would be likely to be challenged robustly.

2.23 Given the common stance of a significant number of EU Member States, including the UK, the Committee may care to consider what options there are to build a consensus behind a proposal for an EU wide requirement for access controls to prevent under-18's being exposed to hardcore pornography. ATVOD has already made such a proposal in its response to the European Commission Green Paper—“Preparing for a Fully Converged Audiovisual World: Growth, Creation and Values”. Rather than setting a test such as “might seriously impair”, which is open to widely differing interpretations, such a measure might simply define hardcore pornography and require each Member State to ensure that media services within their jurisdiction secure that under 18s cannot normally access such material.

Should non-EU VOD services which are targeted at the UK be brought within the scope of regulations designed to protect UK consumers and children?

2.24 As noted in paras 1.8–1.9, a majority of on demand services/websites offering hardcore pornography without effective access restriction operate from outside the EU, notably from the USA and Canada. They are therefore beyond the reach of any European regulator. The exclusion applies even if the service is specifically targeted and marketed at UK consumers.

2.25 Given the large number of such services, and the wide scale of their consumption in the UK, the Committee may care to consider whether consideration should be given to broadening the scope of the relevant UK legislation to enable determinations to be made in relation to VOD services from outside the EU which:

- (a) would be ODPS if the service provider was under UK jurisdiction, and
- (b) are targeted at the UK market?

2.26 Although such a move would raise substantial enforcement issues, it would allow determinations to be made that such services were acting in breach of UK law when hardcore pornographic material is provided without effective barriers to prevent child access. Such a move would send a strong message. It might also encourage UK entities who do business with such services, or who facilitate their provision, to reconsider their relationship with the service provider.

¹⁵⁶ Source: Benchmarking of parental control tools for the online protection of children SIP-Bench II—EU Safer Internet Programme (2011). Key findings, page 22

¹⁵⁷ Source: Ofcom Children and parents: media use and attitudes report (Oct 2011)

¹⁵⁸ Germany, France, Spain (French speaking), Belgium, Italy

Should UK financial institutions refrain from processing payments to non-EU services operating in breach of the Obscene Publications Act

2.27 As noted in para 2.11, Crown Prosecution Service (“CPS”) guidance for prosecutors on the interpretation of the Obscene Publications Act (“OPA”), states that:

“where children are likely to access material of a degree of sexual explicitness equivalent to what is available to those aged 18 and above in a licensed sex shop, that material may be considered to be obscene and subject to prosecution. This applies to material which is not behind a suitable payment barrier or other accepted means of age verification, for example, material on the front page of pornography websites and non-commercial, user-generated material which is likely to be accessed by children and meets the threshold. see R v Perrin, [2002] EWCA Crim 747.”

2.28 The same guidance also advises that:

“There are very difficult jurisdictional issues about whether material hosted overseas is within reach of the English criminal law. It will depend on a range of factors including who posted the material on the site, where it is hosted and what the person intends the material to do. If a web site is hosted abroad and is downloaded in the UK, the case of R v Perrin [2002] 4 Archbold News 2 will apply.

R v Perrin is specifically concerned with ‘publishing’ electronic data under the Obscene Publications Act 1959 and states that the mere transmission of data constitutes publication. It is clear from the decision in R v Perrin and in the earlier case of R v Waddon (6 April 2000 unreported), that there is publication both when images are uploaded and when they are downloaded. In the case of R v Waddon the Court of Appeal held that the content of American websites could come under British jurisdiction when downloaded in the United Kingdom.”

2.29 CPS advice therefore suggests that a US website which offers sexually explicit material which is not behind a suitable payment barrier or other accepted means of age verification is likely to be operating in breach of the OPA if the material is accessed in the UK.

2.30 The Committee might therefore consider whether action might be taken by UK entities which facilitate the provision of such services to UK consumers, for example by processing payments. In this regard, ATVOD notes that while the pornographic services most frequently accessed from within the UK are so-called “tube-sites”, which offer content free of charge, those tube-sites depend for income primarily on driving online traffic to their own or affiliated pay sites. The free content is merely a shop window for services which involve a financial transaction with the user.

2.31 ATVOD has therefore posed to the UK financial industry the question: is it appropriate to process payments to services which, according to CPS guidance, appear to be operating in breach of the OPA? This has been followed by a series of constructive bilateral meetings with key players in the UK financial industry which have in turn led to a summit being held on 10 October 2013, chaired by ATVOD and including senior representatives from The UK Cards Association, the British Bankers’ Association, the Payments Council and a number of leading payment scheme operators.

2.32 ATVOD would be happy to provide the Committee with an update on the summit once it has taken place and to discuss further any of the policy options set out in this submission.

October 2013

Written evidence submitted by Intellect

CHILDREN AND THE INTERNET—THE CONTEXT

Intellect welcomes the Committee’s inquiry into this important matter and the opportunity to provide written evidence. In the context of this inquiry, as the UK’s trade association for the technology industries, Intellect represents a major part of the industrial ecosystem enabling access to the internet: eg, telecommunications operators and Internet Service Providers (ISPs), device manufacturers (PCs, laptops, smart phones, tablets and TVs), operating system providers and security software providers. We also have very good working relationships with content aggregators and technology retailers. As such, we are well placed to provide expert and cross-industry perspectives on this important topic. Our response focuses on online safety for children and the role and contribution of the internet-access industry in enabling a safe internet environment.

Our starting point is that the internet is a good thing. Now entwined in the lives of young people, the internet represents a powerful tool for enhancing their learning, social interaction, and employment, as well as entertainment. The UK enjoys the largest and most vibrant per capita internet economy in the world and its rate of growth is outpacing those of USA and China. The internet enables a more enriched society and a productive economy. Creating an environment online where young people can safely reap these benefits is of paramount importance.

The online environment is an intrinsic part of everyday life. While it has some specific issues and challenges, such as the volume of “instantly” available content, it should not be seen as detached from the physical world and the issues young people face in growing up there. It is essential that online safety issues (eg, illegal content,

inappropriate content and contact, bullying etc) faced by young people is seen as part of and in the context of society's capacity to help them build the confidence, resilience and capabilities to live safe lives and have constructive relationships in the modern world. Technical tools such as parental controls and filters play a crucial role in supporting a safe internet environment and industry has an important role in delivering and ensuring awareness of these tools. However, building of the above resilience and capability in young people requires the constructive collaboration of a range of players from Government to industry, educators, child safety agencies, parents, guardians and children.

ROLE OF INDUSTRY AND PARENTAL CONTROL TOOLS

Consumers and children access the internet through a variety of devices and interconnecting routes. PCs, laptops, games consoles, set top boxes and Connected TVs now enable internet access via the networks provided by domestic (or business) internet service providers. Smart mobile devices (phones and tablets) enable access via mobile operators' networks. Most mobile devices now also enable wifi access via the fixed domestic internet channels and the increasing number of public wifi hotspots. As technological innovation continues apace, the internet access landscape continues to evolve.

It is worth, at this point, to highlight the distinction between the handling of illegal content such as child abuse material and legal content such as adult material which are inappropriate for viewing by children. In the former case, telecommunications operators work with the industry-funded Internet Watch Foundation (IWF) and law enforcement agencies to identify and prevent access to websites with potentially illegal content. They also have procedures for customers to report such sites. In contrast, in the cases of legal but inappropriate content, the focus for industry is to enable parents and guardians to set the boundaries for their children's access to the internet.

In this interconnected landscape, a range of parental control tools, not a single solution, are needed. The internet access industry is highly committed to playing its full part in creating a safe online environment. Apart from the desire to play a responsible role in society, it has a strong additional incentive because without such a safe environment its very market will be jeopardised.

In terms of network operators (fixed and mobile), as stated in the Mobile Broadband Group's written evidence, mobile operators with their January 2004 "UK Code of practice for the self-regulation of new forms of content on mobile" took a proactive stance from the start on online child safety and the availability of content filters—considerably before online safety issues came to the serious attention of Government. Their policy is to apply network filters, for content determined by the British Board of Film Classification (BBFC) as being suitable for adults (18s and over) only. Similarly the main ISPs providing domestic internet access have rolled out parental controls presenting new and existing customers with an unavoidable choice of whether to apply filters or not. These filters cover the whole home, ie apply to all the devices used on a connection and allow parents to choose from a list of content that should be filtered including adult content, extremism and self-harm. Intellect is aware of a continual process to innovate and update these tools for example to enable differentiation between different devices in the home and set different controls depending on the user. Earlier this summer, the six main ISPs providing public wifi access (who are often also providers of domestic internet services) committed to implement filters to block pornography as a standard offering. The Internet Service Providers' Association is now working with some smaller ISPs to understand the issues involved in offering a parental control solution and what alternative approaches could work for them.

Additionally, manufacturers of PCs, laptops, mobile devices and internet connected TVs have been increasingly implementing parental controls on their products. These are intended to complement and reinforce the tools made available by the network operators. One important factor for device manufacturers is that they are largely multinational companies addressing international markets. For them it is essential that parental control solutions implemented on the devices should address multiple markets and not be tailored country by country. The UK's proactive role in promoting parental control tools has given it a lead in Europe and encouraged other countries to consider their approaches. The Government can however do more to encourage other countries to take a similarly proactive stance. Security software providers have also been quick to respond by providing parental controls software either via manufacturers and network operators or directly to consumers.

Thus it is clear that an irreversible momentum has developed across the industrial ecosystem providing internet access to continually develop technology tools in response to the fast evolving internet environment. It is this application of technology innovation which will ensure the diverse set of tools needed to support a safe online environment—not regulation which in contrast could freeze innovation.

Thus we feel that the industrial players have worked exceedingly well in making available the set of technology tools needed and continue to innovate solutions that are of benefit to their customers. Given the availability of a diverse range of tools provided by the industrial players (operators, manufacturers and software providers), a potential area for future focus is to ensure that these tools "dovetail" with each other to maximise complementarity and mutual reinforcement.

EDUCATION AND AWARENESS

As stated earlier, important as they are, parental control tools and filters are only part of the solution in delivering a safe internet environment for children. Ultimately, in a fast changing environment, more effective education and awareness for parents, guardians, educators and children are the only sure ways of providing a holistic and pro-active approach to creating a safe online environment for children and young people.

The 24 June Intellect round table discussion conducted at the House of Lords involving industry, Government, teachers and children's and parent's agencies helped to demonstrate that while there are some excellent initiatives undertaken by companies, agencies and schools, the impact and reach of these education and awareness activities is considerably constrained by a lack of leadership and co-ordination.

Given the interrelatedness of a safe online environment for children with the wider priorities for helping them build the resilience and capability to thrive in modern society, the education and awareness activities (for parents and children) must be tackled holistically—and the leadership and co-ordination for this must come from Government and its agencies.

While the exhortations by Government, for industry to “do more” on parental controls, has at times been helpful in stimulating industry momentum, there is a lack of active leadership on a holistic approach discussed earlier. Furthermore, there has been some confusion as to the role of the Department for Education (now DCMS) and “No. 10” which has not been helpful in terms of providing a clear steer from Government about its policy aspirations in this area.

CONCLUSIONS

Industry has expended considerable resources into the development of parental control tools (including filters) and a variety of tools now exist.

According to Ofcom's 2013 Report, “Children and Parents: Media Use and Attitudes”, 83% of parents say they trust their child to use the internet safely and 85% of parents use a combination of interventions ranging from parent-child discussions to the application of parental control tools. While this is a healthy sign, the focus now should be about driving these numbers up even further through education and awareness.

While the Government's recent focus on online child safety has been helpful in driving up public debate on the issues as well stimulating further industry momentum on technology solutions, we feel that the climate of public discussion and Government stance should change from one of “industry should do more” to facilitating a constructive dialogue which recognises and supports the good work undertaken voluntarily often in best practice partnerships with trusted bodies such as the BBFC and IWF.

Government has an important leadership role in creating the partnerships for a holistic approach to enabling a safe online environment for children and providing clear consistent guidance to industry on its expectations. There needs to be clear and adequately resourced lines of policy responsibility with consistency of Government approaches to avoid the at times fragmented Government approach. Industry will be more than a willing partner.

The climate of public discussion needs to change from admonishing industry for not doing enough to one of positive collaboration.

ABOUT INTELLECT

Intellect is the trade association for the UK technology industry. In 2007, the industries Intellect represents accounted for 8% of UK GDP, £92bn of Gross Added Value and employed 1.2 million people.

Intellect provides a collective voice for its members and drives connections with government and business to create a commercial environment in which they can thrive. Intellect represents over 750 companies ranging from SMEs to multinationals. As the hub for this community, Intellect is able to draw upon a wealth of experience and expertise to ensure that its members are best placed to tackle challenges now and in the future.

Our members' products and services enable hundreds of millions of phone calls and emails every day, allow the 60 million people in the UK to watch television and listen to the radio, power London's world leading financial services industry, save thousands of lives through accurate blood matching and screening technology, have made possible the Oyster system, which Londoners use to make 28 million journeys every week, and are pushing Formula One drivers closer to their World Championship goal.

In response to a request by Government Ministers in late 2011, Intellect established industry working groups covering the fixed, mobile and (most recently) the connected TV environments with a view to developing cross-industry approaches on parental controls. Through these activities we have played an industry leadership role in promoting better understanding within industry and between industry and Government on parental controls and online child safety activities. In recognition of this role, Intellect's Director General, Mr. Julian David has been recently invited to join CEOPs Strategy Group, as its industry representative.

October 2013

Written evidence submitted by Telefónica UK Ltd

1. O2 is the commercial brand of Telefónica UK Ltd, a leading digital communications company. O2 in the UK has over 23 million customers and runs 2G, 3G and 4G networks. The company also operates O2 Wifi, which provides over 9,000 free wifi hotspots and has over eight million customers across the UK. Telefónica UK Ltd owns half of Tesco Mobile and has over 450 retail stores. The company is part of Telefónica Europe plc (a business division of Telefónica SA), which uses O2 as its commercial brand in the UK, Slovakia, Germany and the Czech Republic.

2. Telefónica UK Ltd (Telefónica) is a member of the UK Mobile Broadband Group (MBG), which has separately submitted evidence to the Select Committee on behalf of our industry. This paper is an additional submission on behalf of Telefónica. Although the inquiry will consider a range of issues relating to online safety, this paper is primarily concerned with that part of its terms of reference that is focused on “how best to protect minors from accessing adult content”.

3. Telefónica does not believe there is a “silver bullet” solution that will address every issue and challenge relating to online safety, many of which will evolve rapidly over time through advances in understanding and technology, as well as changes in online behaviour. No technology can be a full substitute for parental responsibility, which is vital to the overall task of ensuring online safety. In addition, while there is widespread agreement on the need to protect children from inappropriate online content, there is no such consensus on how this can be achieved and what the exact roles should be of, for example, parents, schools, IT companies, statutory regulation etc.

4. The “internet industry” is at times referred to as having a collective responsibility for online safety. Telefónica does not shirk its own responsibility and believes that collaboration on this issue across the industry is vital. However, Telefónica believes also that it is important to understand the distinctive role and actions of mobile network operators within the broader industry.

5. *Illegal Content.* Telefónica is a longstanding member of the Internet Watch Foundation (IWF) and sits on its board. We have, therefore, a long track record of involvement in its work. We support its new focus on proactively hunting out and removing illegal images from the internet and have committed additional funding to the organisation to help it fulfill this revised and expanded brief. We block internet access to the IWF master-list of illegal websites not just from O2 mobile phones but also from O2 Wifi (see below). For a number of years we have deployed “splash” pages to explicitly warn customers if they seek to access an IWF blacklisted site. In addition, this summer O2 promptly implemented the new IWF splash-page co-authored by the Lucy Faithfull foundation in support of the Stop it Now! campaign. This splash-page may be accessed at <http://wap.o2.co.uk/iwfblock>.

6. *18+ Content.* All 18+ content is placed behind an Age Verification (AV) “shield”. A customer cannot get access to 18+ content on an O2 mobile phone unless he/she successfully completes this AV process to prove they are aged 18 or over. The AV process is based on the MBG-led British Board of Film Classification (BBFC) Framework.

7. *Parental Controls.* Our free Parental Control service limits the websites that children can access on their mobiles. It only lets them access sites that have been classified as suitable for children under 12 years old. Parental Controls are easily applied, with guidance and instruction available online, in-store and by telephone from our customer service team. When customers purchase a phone, they are asked if the phone is for a child and if they would like the Parental Controls switched on at the point of sale.

8. *Education & Information.* We are committed to establishing and maintaining a dialogue with parents and young people to increase their awareness and knowledge of the safety tools available and the behaviours they need to adopt to maximise online safety. For example, in August O2 sent SMS messages to all of its consumer customers, inviting them to *Staying Safe*—an online portal where they can learn of online and mobile safety issues and be provided with some practical help and advice. This campaign has been O2’s biggest SMS campaign to date. *Staying Safe* highlights topics requested by our customers, such as what content we block, think before you post, online bullying, phishing or scam emails, how to spot a scam email, keep your money safe; in-app purchases and protect your phone. O2 also has a dedicated website for parents (<http://www.o2.co.uk/parents>); and we have published and distributed the book “Who WNTs 2 No” to schools and libraries. This book aims to teach children not to share their personal information online using funny characters and children’s language. It has also been released as an application available free on Apple devices from iTunes. We are also long term supporters of Safer Internet Day and participate in its activities; we produce an “Advice to Parents” booklet that is available in-store; we have made use of child safety pledge cards in the past; we have trained people in our business as “digital ambassadors” who have then visited schools to run online safety sessions; we undertake child safety research among our customers; and do focus group research work with partners such as Mumsnet. We also have a link from our website to ParentPort.

9. *O2 Wifi.* O2 Wifi was launched in 2011 and provides free public wifi to our own customers and those of other networks on the London Underground, Canary Wharf and many restaurant and store chains, including McDonalds, Costa Coffee, All Bar One, Subway, Toni & Guy, Debenhams and Café Rouge. All 18+ content is blocked on O2 Wifi, including the IWF list, on O2 Wifi, which also has a default safe search engine setting. These features are standard and free.

10. *Public Policy.* In addition to our involvement with the IWF and Mumsnet (see above), we have regular dialogue with organisations such as the Child Exploitation & Online Protection Centre (CEOP), Childnet, the Children's Charities Coalition on Internet Safety etc and are founder members of the CEO Coalition (to make the internet a better place for kids), established by the European Commission in 2011. We have also been founding participants of UKCCIS with representation on the UKCCIS Board. We have regular contact with Ofcom, PhonepayPlus, the Office of Fair Trading, the Information Commissioner's Office, the DCMS, Home Office and Department for Education on child safety issues. Our commitment to policy engagement, therefore, has been and remains very strong, but there are many issues and bodies to deal with.

11. Telefónica also offers the following observations on the key issues and challenges in the field of online safety:

International. Sexual child abuse images on UK based URLs are typically removed from the internet within 60 minutes of the IWF learning of their existence. However, about 99% of such images are hosted in other countries, so a huge amount of work is required by foreign and international agencies to make a strong impact on the problem. This is an international issue, not one specific to the UK. In our view, therefore, the government needs to show strong leadership in working effectively with international regulators and other governments to ensure there is cross-border coordination and action. This requires policies in favour of internet standards and enforcement.

Enforcement. It seems that the flow of work from identifying illegal content to prosecution needs to work smoother. The proactive approach now being taken by the IWF will deliver more intelligence to CEOP on victims and criminals. The investigative and prosecution authorities will require a level of resource to manage this increased workload. We need a higher number and rate of prosecutions to increase the efficiency, actual impact and value that is being delivered to act as a further and stronger deterrent. On both enforcement and prosecution a greater level of international cooperation and action is required. Inter-governmental summits need to put this on their agenda for pragmatic action.

Online/Offline harmonization. While Telefónica and other operators operate a robust system of age verification to ensure the safeguarding of under-18s from adult internet content, many offline vendors are not as effective and vigilant in this regard. Perhaps it is time to insist that *all* publishers in the UK—online or offline—should have the same UK legal obligations to protect children from being exposed to inappropriate images and content.

Education and skills. We are committed to supporting and encouraging digital skills and entrepreneurship in young people through such initiatives as Campus Party and the Think Big School (which will work with over 3,000 14–18 year olds this year). We are looking at how we can incorporate online safety messages into the Think Big School schedule, but the government's new computing and D&T curricula offer a good opportunity for online safety messages and content to reach many more young people.

Devices. Telefónica cannot fully control the human factors (HMI) or ease of use on devices. Many devices and Apps are purchased through independent channels or Apps stores. It is important that devices approved for connection to the internet meet essential requirements and that Apps are deemed legal. One avenue that could be considered is whether we have the right Type Approval procedures to assure internet safety, pragmatic HMI controls and trusted Apps.

12. In conclusion, there is a lot of goodwill and effort already being exercised in support of online safety. Telefónica and other mobile operators have a strong track record of commitment and achievement in this area. New challenges and players are bound to emerge, of course, and to help ensure online safety is effectively addressed, a partnership approach is required between industry, government, charities and parents. In the UK Council for Child Internet Safety (UKCCIS) a body already exists that can bring together the range of stakeholders needed to make a coordinated and sustained contribution to delivering online safety.

September 2013

Written evidence submitted by the National Centre for Cyberstalking Research (NCCR)

- Protecting children from accessing content requires enhanced identification and authentication schemes.
- Education has a vital role to play in all strands and requires adequate funding.
- There needs to be greater responsibility and action by providers of Social Media Services to protect their users.
- Anonymity on the Internet can lead to disinhibited behaviour and actions that victims find distressing.

BACKGROUND

1. The Internet is an excellent vehicle that allows enhanced communications enabling a more cohesive society and more productive business world. However, there are a number of serious issues that have arisen in this communications network, and further legislation and regulation are needed to ensure the safety of a number

of groups. The National Centre for Cyberstalking Research (NCCR) was established to address the need for research and analysis into the motivations, means, impact and investigation of cyberstalking. This submission to the call for responses to the Culture, Media and Sport Committee inquiry into Online Safety predominantly relates to matters around online grooming and stalking. Professor Maple has also contributed to the submission by the BCS.

HOW BEST TO PROTECT MINORS FROM ACCESSING ADULT CONTENT

2. It should be recognised that there is a fundamental difficulty in current computer systems access. That is, that a user usually presents an identity (username) and access credential (password, biometric, token or other). Whoever possesses this information can, in general, access authorised information. Given the acceptance that there is adult content on the Internet, any minor with appropriate credentials could access that content: those minors that are suitably determined will be able to access material intended only for adults. Society must make it virtually impossible for minors to unintentionally access adult content, and difficult for minors to access adult content that they have actively sought.

3. There is a need for clarity about the role of parents in “parental controls”. Many parents are unaware of what is their responsibility and what is the responsibility others. Many families that we have met, even with “filters” and “controls” in place, are sure their children have access to material not intended for minors. They are unaware of what they can do to prevent such access.

4. There is a problem regarding the understanding, by children, of what is adult content. Whilst with games, films and even music there may be some classification of the content, that does not exist for a great deal of information and content on the Internet. Furthermore some “adult” (and indeed illegal) content is actually *produced* by children (in the form of sexting for example). The Internet Watch Foundation (IWF) has stated that 12,224 images, apparently created by minors, were reported in just four weeks.

5. Content (illegal, adult or otherwise) can spread around the internet very rapidly and so removing material from one site may have minimal impact if the material has already been harvested and reposted to another site.

6. While awareness is important, education is also necessary. The technical knowledge of children is very impressive, but there is a need to educate children on the impact of technology and the management of information in the unregulated space that is the Internet. There is good guidance available through initiatives such as Safer Internet and Get Safe Online. A particular area that requires special attention in any education programme is the spread and the permanence of material put online.

7. It is not only children that require educating, but also parents. Parents use the Internet in different ways to children and therefore may not understand how best to protect their children. It is unlikely as many parents have seen Chat Roulette as children have. Children consider email outdated and use Youtube not only to access videos but as a discussion medium. It would be positive for schools to be involved in the bringing together of parents and children. Topics that could be discussed include the management of online relationships, appropriate communications (sending and receiving) and what to do if children are concerned by interactions online.

FILTERING OUT EXTREMIST MATERIAL, INCLUDING IMAGES OF CHILD ABUSE AND MATERIAL INTENDED TO PROMOTE TERRORISM OR OTHER ACTS OF VIOLENCE

8. There are two main types of method that can be employed to filter material; material can be filtered by automatic or manual means. The former relies on sufficiently sophisticated algorithms to detect unwanted material and the latter relies on people in the community notifying an authority of the existence of unwanted material. Such material is then removed, and an identifier placed on a blacklist so that the material cannot enter a site again.

9. The difficulties in blacklisting material should be recognised. Automated tools are not yet sufficiently advanced to perform blacklisting without some human control. An Irish study considering filtering within a school setting found that 50% of schools reported that filtering occasionally blocked valid educational sites, while 20% of schools reported that it regularly did so. (<http://tnc2007.terena.org/programme/presentations/show4fa0.html>). Hence it is difficult to rely on content based automated tools alone. Furthermore, what should be restricted and what should pass through a filter is often a judgement call and so some level of human intervention is likely to be required.

10. Blacklisting is an important activity but does come with a cost, both financial and non-financial, that must be met. Currently, for example, the Internet Watch Foundation, is largely funded by ISPs. This model would need to continue, but it may be possible to consider other routes for funding filtering technologies in the general sense. The value of the time of the volunteers that report material to the IWF is not insignificant, and must be understood. It is vital that reporting of unwanted material is a simple and transparent process. The True Vision initiative for hate crime reporting is an excellent example of a simple and transparent reporting mechanism, but it needs to be more widely publicised.

11. Consideration could be given to requesting the Internet Watch Foundation to widen its remit—this could have the benefit of a one-stop reporting centre.

PREVENTING ABUSIVE OR THREATENING COMMENTS ON SOCIAL MEDIA

12. The issue of abusive or threatening comments on social media has clearly been one that has disturbed society of late and gained major press coverage. In particular, the case on Twitter of Caroline Criado-Perez received major attention and highlighted this negative side of the new communications environment we live in. In response to the case, Twitter did state it would trial a “Report Abuse” button. There is no such button available on Twitter at this time and this resistance by the social media companies to protect its users and provide an avenue for reporting requires addressing. Research undertaken by the NCCR has shown that people do not know where to report cyberstalking abuse, or who should be responsible.

13. Some social media providers do provide a Report Abuse button, but it is important that they also provide clear guidance and support for victims of distressing communications. These should detail methods for locating support and information on how to report the incident(s). Where possible and appropriate providers should maintain regular contact with support and criminal justice agencies.

14. The Guidelines on prosecuting cases involving communications sent via social media from the Director of Public Prosecutions published on 20 June 2013, categorise communications as those which:

- (a) amount to threats of violence;
- (b) target an individual and amounts to harassment or stalking within the meaning of the Protection from Harassment Act 1997 (including two new criminal offences of stalking were added as sections 2A and 4A to the Act by the Protection of Freedoms Act 2012);
- (c) amount to a breach of a court order;
- (d) those not covered by the provision above but may be considered grossly offensive, indecent, obscene or false.

15. The distinction between the cases is very important to ensuring the correct legislation, if any is used in cases of threatening or abusive communications. In particular, given the evidence of the significant impact of the first three categories (including recent evidence on the impact of cyberstalking) we must ensure that such actions are not simply considered as grossly offensive. This would, however, be the easiest route for many stakeholders to take and therefore should be guarded against.

16. Without the public having a clear understanding of the differences in these communications the problem is unlikely to diminish. Digital Natives have embraced technology but unfortunately without appropriate training and education they struggle to understand the social norms of internet communication and behaviour. Education surrounding the appropriate use of these new communications media will have an important role to play in combating the problem.

17. There is a clear issue around anonymity and perceived anonymity (as well as untraceability) in social media.

- (a) In cases where senders of malicious communications have anonymity and (practical) untraceability there can be difficulty in bringing justice and technological and legal changes may be needed.
- (b) In cases where senders have a (mistaken) perception of anonymity or untraceability they may display fewer inhibitions and feel beyond reproach. It is important that all those that can assist in making communications more traceable, particularly by giving up log information, do so fully and readily when requested by those in the criminal justice system. The recent changes to the Protection from Harassment Act 1997 do give police further powers and this is a welcome change.
- (c) Where receivers of abusive messages perceive (rightly or wrongly) anonymity or untraceability of the senders they may feel there is little point in reporting the communication, even when it has significant impact.

18. It is important all stakeholders consider the vulnerability of the victim in cases of abusive or threatening messages.

September 2013

Written evidence submitted by Ethos Capital Ltd

SUBJECT: THE POST OFFICE COULD BE AT THE FOREFRONT OF INTERNET SAFETY

SUMMARY

- There are several aspects of online safety that are raising concerns.
- There are advantages to establishing proper links between “online identities” and “real-world identities”.
- We have developed a Service that aims at solving some of the concerns about online safety by utilising the Post Office’s vast network of branches across the UK.

- We sent a proposal to the Post Office to implement this Service. The proposal included paragraphs 4, 5 and 6 below. A version of these paragraphs is also published on our website.
- We decided to share the below information with your Committee in the event that you find it useful to the Inquiry into Online Safety.

DETAILS

1. The Culture, Media and Sport Committee is investigating a number of aspects of online safety that are currently raising concerns, in particular:
 - (1) How best to protect minors from accessing adult content;
 - (2) Filtering out extremist material, including images of child abuse and material intended to promote terrorism or other acts of violence; and
 - (3) Preventing abusive or threatening comments on social media.

2. We have recently developed a Service that aims at addressing points (1) and (3) above by utilising the Post Office's vast network of branches across the UK.

In addition, this Service would make it more difficult for sex offenders to pose as teenagers on social networks to deceive their targets.

Furthermore, this Service would facilitate the realisation of the Parliament 2.0 vision that was announced recently by the Speaker, Mr John Bercow, and which involved E-Voting. This is because E-Voting requires establishing proper links between "online identities" and "real-world identities".

3. We sent a proposal to the Post Office to implement this Service. The proposal included a version of the following three paragraphs. We are currently awaiting their response on whether they would like to approve this Service so we can launch.

4. **Existing Problems**

- (1) Minors can easily access adult content.
- (2) Sex offenders pose as teenagers on social networks to deceive their targets.
- (3) Abusive and threatening comments by anonymous users on social media.

5. **Solution**

The simplest and most robust solution to the above problems is to find a way to reliably and systematically verify the age of Users when visiting certain websites and, at the same time, to protect their privacy.

This can be easily done using a unique code that is issued based on a face-to-face and ID verification and then used regularly by Users when visiting certain websites.

We are suggesting utilising the Post Office's vast network of branches across the UK to verify the age of Users so Users can generate these unique codes automatically.

6. **Implementation**

We have developed a website that enables each authorised Post Office employee to verify the age of any User who presents a valid ID in person. This verification enables the User to generate a unique Code online.

If the User would like to visit a third-party website that requires age verification, they can enter this generated Code on that website. This Code will then be authenticated by our servers without revealing the name or details of the User as we don't hold this information.

Therefore, third-party websites will be able to grant access to real Users with the appropriate age, at the same time that the privacy of these Users will be protected. Furthermore, for additional safety, Users (or their parents) will receive an email or an SMS notification each time the Code is used.

The Post Office can charge a fee for verifying the accounts of Users in a similar manner to how it processes passport applications.

7. Additional information could be found at www.netpasscode.com or by contacting us at the details outlined in the header of this document.

December 2013