



House of Commons

Culture, Media and Sport Committee

Online safety

Sixth Report of Session 2013–14

Volume I

Volume I: Report, together with formal minutes, oral and written evidence

Additional written evidence is contained in Volume II, available on the Committee website at www.parliament.uk/cmscom

*Ordered by the House of Commons
13 March 2014*

HC 729

Published on 19 March 2014
by authority of the House of Commons
London: The Stationery Office Limited
£20.00

The Culture, Media and Sport Committee

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

Current membership

Mr John Whittingdale MP (*Conservative, Maldon*) (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

Contents

Report	<i>Page</i>
Summary	3
1 Introduction	6
2 Child abuse images	8
Nature and scale	8
The law	9
Enforcement	10
Surveillance	12
Internet service providers	14
Internet Watch Foundation	15
Deterrence	16
Other material	17
3 Adult content	19
Nature and scale	19
The law	20
Enforcement	21
Age verification	24
Site blocking	26
Filters	27
Media literacy and education	31
4 Social media	34
Nature and scale	34
The law	35
Enforcement	36
Reporting	39
Advice and support	40
Anonymity	42
Formal Minutes	48
Witnesses	49
List of printed written evidence	50
List of additional written evidence	50
List of Reports from the Committee during the current Parliament	52

Summary

The internet has revolutionised communications and information sharing. It provides an ever increasingly important platform for creativity and economic growth. Online social media services are providing new ways of interacting and keeping in touch. Online communications enable expressions of human behaviour both positive and negative; sometimes downright criminal. Our inquiry has focused on three disparate aspects of online content and behaviour, all of which are of widespread concern: illegal content, especially images of child abuse; harmful adult content being made freely available to children; bullying and harassment on social media.

Both the publication and possession of child abuse images are rightly illegal. While these offences are bad enough, it must not be forgotten that such images represent crime scenes, often of the most horrific kind. There is a clear need to ensure that the police have adequate resources to track down and arrest online paedophiles in sufficient numbers to act as a meaningful deterrent to others. If necessary, additional funding should be provided to recruit and train a sufficiently large number of police officers adequate to the task.

The Child Exploitation and Online Protection (CEOP) Command, now part of the new National Crime Agency, has a well-deserved reputation as a lead body in tackling child abuse. It has been increasingly effective not least because it is not solely a criminal justice organisation: its education and social care work has also been very important in increasing public understanding of the problem of child abuse and in offering means of countering abusers. All three elements of its mission – education, social care and criminal justice – need to be actively pursued and publicised.

The Internet Watch Foundation, too, has played a crucial role in removing and blocking child abuse images online. We very much welcome their new commitment to embark on proactive searching for online child abuse images. The sooner these can be found and removed, the better. However, we are concerned that the additional staff resources being allocated to this task could prove woefully insufficient to achieve substantial progress towards what must be an important intermediate goal: the eradication of child abuse images from the open internet. Tracing paedophiles who share images on peer-to-peer networks and the so-called hidden internet continues to challenge both the police and the internet service providers; it is a challenge that, by working together, they must overcome.

Legal adult pornography is widely consumed. This includes explicit “hard core” material that attracts an R18 certificate from the British Board of Film Classification. Parents and carers clearly have a key role, not to mention interest, in preventing harmful material of this kind becoming available to children. However, they should have access to more information and help where and when they need it. In the off-line world, it is the newsagent, not the parent, who voluntarily places some adult magazines on a top shelf out of reach of children. It is the local authority, not the parent, which administers the licensing of sex shops selling R18 pornography to which children may not be admitted. Some level of analogous protection ought to be provided in relation to online material. At the moment,

little is.

Legal adult sites could restrict access by children in a number of ways. In general a robust age verification process should be in place; as part of this, sites could use a combination of the following: requiring payment by a credit card linked to an adult; shielding the content behind a warning page; attaching metadata to the website to make it easier for filters to operate and for search engines not to return the material when operating in a safe search mode.

Filters may not be failsafe, but they continue to improve and are an important way of protecting children from harmful content. We very much welcome the introduction of whole home filtering solutions that prompt account holders with a choice to apply them. The main internet service providers should have contacted all their customers by the end of the year to offer this valuable service. We want to see all other ISPs following suit.

Publishing adult pornography in a way that makes it readily available to children is likely to be an offence under the Obscene Publications Act 1959. We do not believe the police should be deterred from bringing to book publishers of adult pornography who make little attempt to shield children from their product. While acknowledging that the enforcement of obscenity legislation is fraught with difficulty, not least in the context of the internet, we believe there is scope for greater enforcement in this area to provide some deterrent effect. There may also be scope for blocking particularly harmful adult websites that make no serious attempt to hinder access by children.

As part of its existing media literacy duties, Ofcom has an important role in monitoring internet content and advising the public on online safety. However, we are anxious to avoid suggesting a significant extension of formal content regulation of the internet. Among the unintended consequences this could have would be a stifling of the free flow of ideas that lies at the heart of internet communication. Rather, more needs to be done to signpost the advice and educational resources available to both parents and teachers. This is all the more pressing given the growing use of social media and its misuse by some – both adults and children. Today, one in five 12–16 year-olds think being bullied online is part of life.

Social media providers should offer a range of prominently displayed options for, and routes to, reporting harmful content and communications. They should act on these reports expeditiously, keeping the complainant and—where appropriate—the subject of the complaints informed of outcomes and actions. Given that Facebook and Twitter are aware of the extent to which their services are accessed by younger children, thanks to age verification processes that are at best flimsy, we expect them to pay greater attention to factoring this into the services provided, the content allowed and the access to both. The same applies to other social media companies in a similar position.

Some of the worst online bullies and trolls are being brought to book in the courts. Much of the abuse and bullying that takes place online is covered by existing laws, but these need to be clarified with guidance updated for the online space. Young people especially are distinguishing less and less between their lives on the internet and in the real world. Bullying that takes place in the playground can merge seamlessly with bullying on smart phones and tablets. Sometimes this ends with the tragedy of teenage suicide. It is just one

reminder that staying safe off-line includes staying safe online too.

1 Introduction

1. The internet is changing the way we communicate and modifying the way we behave. A wealth of information and a platform for myriad interactions, it is fostering creativity and economic growth on an unprecedented scale. Sadly, inevitably, the darker side of human nature finds expression too: in the commissioning, distribution and viewing of illegal images of child abuse; in adult material unshielded from children's eyes; in threatening and abusive messages via social media. In the belief, sometimes mistaken, that the internet offers anonymity, trolls and bullies hound adults and children alike, often with tragic consequences. The internet can amplify the pack mentality of the unthinking.

2. With these disparate concerns in mind, we decided to launch an inquiry into online safety, taking care in our terms of reference to keep distinct three very separate aspects:

- How best to protect minors from accessing adult content;
- Filtering out (i.e. blocking and removing) 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.

3. We took oral evidence from the following: John Carr, Secretary, Children's Charities' Coalition on Internet Safety; Claire Lilley, Senior Analyst, NSPCC; Anthony Smythe, Managing Director, BeatBullying; Susie Hargreaves, Chief Executive, Internet Watch Foundation; Peter Davies, Director, Child Exploitation and Online Protection (CEOP) Command, National Crime Agency; Stella Creasy MP; Nicholas Lansman, Secretary General, Internet Services Providers' Association; Dido Harding, Chief Executive Officer, TalkTalk Group; Hamish Macleod, Chair, Mobile Broadband Group; Jim Gamble, Independent Chair, City and Hackney Safeguarding Children Board; Simon Milner, Policy Director, UK and Ireland, Facebook; Sinéad McSweeney, Director, Public Policy, EMEA, Twitter International Company; Tony Close, Director of Content Standards, Licensing and Enforcement, Ofcom; Claudio Pollack, Group Director, Content Consumer and External Affairs Group, Ofcom; Rt Hon Damian Green MP, Minister of State for Policing, Criminal Justice and Victims; Edward Vaizey MP, Parliamentary Under-Secretary of State for Culture, Communications and Creative Industries; Claire Perry MP, Special Adviser to the Prime Minister on Preventing the Commercialisation and Sexualisation of Childhood.

4. Many other organisations and individuals submitted written evidence, among them charities representing children and young people. Nevertheless, we felt it important to engage directly with young people themselves. We were therefore grateful to the following charities which, together with parents, organised a visit to the House of Commons by eight young people ranging from ages 16 to 25: Childline Services, CARE,¹ Childnet International, Porn Scars, Safermedia and Brook. The young people each gave us compelling and, at times, harrowing accounts of the harmful experiences they had endured as a result of online bullying and access to age-inappropriate material, particularly adult

pornography. We are very grateful to them for speaking to us and, indeed, to all who provided evidence to our inquiry.

2 Child abuse images

Nature and scale

5. Both the publication and possession of child abuse images are illegal. This is one form of censorship that commands near universal support. Not only do such images represent actual crime scenes, but they are likely to be used by online paedophiles to encourage and legitimise their criminal activities. The law in the UK recognises this by proscribing a range of images of different types, whether photographic or not.

6. Estimating the scale of child abuse images on the internet is problematical given the secretive nature of much online activity by paedophiles. The term “child pornography”, while still in common use, not least in legal texts, is now largely abjured by professionals working in child protection. In no way can images of this kind be likened to consensual activities depicted in legal adult pornography. Paedophiles ought to be denied any comfort when seeking to affirm their practices and preferences. Accordingly, we shall use the terms “child abuse images” or “child sexual abuse images” to refer to the material covered in this section of our report. Claire Lilley of the NSPCC told us:

We need to educate people that these are not just images; that by looking at these images, they are committing an offence; that a child is being re-victimised every single time an image is looked at; and that they are potentially affecting their own sensitivity around the issue and escalating their own ability to go down that route and end up abusing in the physical sense themselves. There is quite a lot of research now about the crossover between non-contact and contact offending and CEOP would put it at about 50%. There are a couple of studies that put it at between 40% and 55%, which is a very high level of crossover. It is not just looking at an image; it is much more dangerous than that.²

Peter Davies of CEOP underlined this point: “anybody who possesses indecent images of children is a criminal, but is also somebody who might present an additional risk to children, as if that were not enough.”³

7. As the NSPCC notes, child abuse images are a visual record of the sexual abuse of a child. They can include pseudophotographs, animations, drawings, tracings, videos and films which are being streamed live. In the UK images are graded on a 1–5 scale. Level 5 images involve sadism or bestiality, Level 4 will portray a child engaged in penetrative sexual activity and so on to Level 1, where the images will depict erotic posing with no visible sexual activity.⁴ In 2012 the NSPCC issued FOI requests to every local police force in England and Wales asking them to state how many child abuse images they had seized in arrests made in the two years ending April 2012. The five police forces (none of which had a large metropolitan base)⁵ that replied had seized over 26 million such images. The

2 Q 29

3 Q 34

4 Ev 70

5 Q 5

Children's Charities' Coalition on Internet Safety told us that, on one calculation, that would imply that over 300 million illegal images may have been seized by all forces over the same period.⁶ Many of the images seen by the Internet Watch Foundation have been recycled, though one or two new images—each representing a new victim—are seen weekly.⁷

The law

8. Section 1 of the Protection of Children Act 1978 makes it a criminal offence to take, permit to be taken or to make, distribute, show, advertise or possess for distribution any indecent photograph or pseudo-photograph of a child under the age of 18. Simple possession by individuals is proscribed by the Criminal Justice Act 1988. The 1978 Act defines a pseudo-photograph as “an image, whether made by computer-graphics or otherwise howsoever, which appears to be a photograph.” Pseudophotographs were brought within the ambit of the Act by dint of the Criminal Justice and Public Order Act 1994. The Criminal Justice and Immigration Act 2008 extended the definition of an indecent photograph to include a tracing or other image derived from a photograph or pseudophotograph. Part 2, Chapter 2 of the Coroners and Justice Act 2009 extended the law proscribing the possession of child pornography to include non-photographic images such as cartoons, drawings and computer-generated images.

9. Peter Davies of CEOP told us: “it is quite remarkable to me how far the criminal legislation, for example, around indecent images of children, which was, I believe, conceived and passed before the internet was around, has still pretty much stood up to the new world of child abuse online, and I do not think what we need is a basic root-and-branch piece of work.”⁸ He added that “the UK has just about the best suite of child protection legislation that there is, and that we are more of an example to others than we are in need of catching up.”⁹ At a recent discussion meeting of the Digital Policy Alliance, the Deputy Director of CEOP Command, Andy Baker, referred in general terms to child protection legislation more widely; he suggested it would be better to “tidy it up”.¹⁰ The fact that the Communications Act 2003 was drafted with no mention of the internet also should be addressed. **We believe that the Government should, in due course, consolidate the law around child abuse images into a single Act of Parliament with a view to providing even greater clarity for the purposes of law enforcement and deterrence.**

10. Clearly the fight against child abuse and child abuse content on the internet is an international one. Peter Davies referred to two conventions—the Budapest Convention and the Lanzarote Convention—which together aim to provide a legal framework for protecting children online. The Budapest Convention on Cybercrime¹¹ and the Lanzarote Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse¹²

6 Ev 66

7 Qq 34-35, 40

8 Q 48

9 Q 48

10 Recent Developments in Child Internet Safety, Digital Policy Alliance Discussion Meeting, 22 January 2014

11 <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG>

12 <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=201&CM=1&DF=&CL=ENG>

are both Conventions of the Council of Europe. The United Kingdom is a signatory to both, though it has ratified only the former. Last July, the Parliamentary Under-Secretary of State, Home Office (Lord Taylor of Holbeach) was unable to say when the Government expected to ratify the Lanzarote Convention; he said: “Until the work to assess the practical arrangements is complete, it will not be possible to confirm the timescales for ratification. That work remains ongoing.”¹³ **Given the worldwide nature of online crime, we recommend that the Government press for wider international adoption of both the Budapest and Lanzarote Conventions. The Government should ratify the Lanzarote Convention as soon as practicable.**

Enforcement

11. Peter Davies of CEOP referred to an assessment, published in June 2013,¹⁴ which gives an estimate of around 50,000 people in the UK who commit child sexual abuse offences “at least to the level of possessing indecent images of children.”¹⁵ He went on to tell us that the highest volume of offenders are using peer-to-peer networks rather than the open internet. “Far fewer” offenders are using the hidden internet, “also known as Tor or The Onion Router or something similar.”¹⁶

12. The proliferation of material which is illegal in all circumstances poses a particular threat and a range of challenges, not least to law enforcement. John Carr of the Children’s Charities’ Coalition on Internet Safety referred to the challenge posed by the scale of online child sexual abuse: “I think it is a profound shock to realise that so many people are interested in that type of material. There is an appetite for it and people go and get it, and they circulate it. They are getting away with it because we do not have the capacity to stamp it out.”¹⁷ Peter Davies of CEOP referred to a need for “a plan that goes beyond enforcement”.¹⁸ That is not to diminish the vital role that law enforcement must continue to play. The former chief executive of CEOP, Jim Gamble, emphasised the need to deter paedophiles by applying the law as it currently stands.¹⁹ Citing figures given by Peter Davies, Jim Gamble said:

On the 50,000 Peter talks about, those are peer-to-peer sites. Those are hard-core paedophiles who do not stumble across anything on Google. They nest in these places on the internet where they can share secretly. You have to infiltrate that. You have to infiltrate it. You have to identify who they are and follow them offline and arrest them.²⁰

13. He went on to propose the recruitment, by each police force, of up to ten special constables to work online. Their job would be to seek out online paedophiles with the aim

13 HL Deb, 24 July 2013, col 197WA

14 http://ceop.police.uk/Documents/ceopdocs/CEOP_TACSEA2013_240613%20FINAL.pdf

15 Q 40

16 Q 43

17 Q 27

18 Q 59

19 Qq 114, 116

20 Q 114

of achieving arrests in sufficient numbers to have a significant deterrent effect.²¹ Mr Gamble puts a cost of £1.4 million on setting up such a scheme which would include the recruitment of 12 detective sergeants and 12 trainers and coordinators.²² He told us: “If you did that, you would have 520 people online at any given time who could manifestly cover 10, 20, 30 or 40 chat-room environments, where you would have people out there protecting our children. Not rogue vigilantes, but properly vetted, properly trained and accredited and properly supervised officers online. To me, that is what we should be thinking about so we attack the root cause, which is people.”²³

14. CEOP (Child Exploitation and Online Protection) is now one of the four commands within the National Crime Agency, which commenced on 7 October 2013. The CEOP centre has existed since 2006 and was previously affiliated to the Serious Organised Crime Agency. Peter Davies told us: “Our mission, whether as a centre or as a command, as we are now, is to protect children from sexual exploitation and sexual abuse. When we were founded, there was heavy emphasis on online protection. Our remit does not limit us to online activity, but what we try to do is to become a national hub for intelligence, a national contact point and a source of expertise and specialist support on any aspect of child sexual exploitation that would benefit from that approach.” Mr Davies also highlighted the contributions being made by online child protection units in UK police forces.²⁴

15. In its evidence, the Home Office praised the Child Exploitation and Online Protection Command of the National Crime Agency for both its operational work and educational programmes. In 2012/13 CEOP received an average of 1,600 reports per month of abuse from the public and the internet industry, a 14% increase on the previous year. “CEOP maintains close relationships with a wide range of stakeholders from law enforcement, industry and the educational sectors nationally and internationally.”²⁵ In 2012/13, CEOP protected 790 children from sexual abuse, an increase of 85% on the previous year, and its work led to the arrest of 192 suspects.²⁶

16. According to the Home Office, the CEOP budget “has effectively been protected in cash terms since 2011/12” and “there are now more people working in CEOP than at any time in its history”.²⁷ The Home Office also states that becoming part of the NCA will bring advantages to CEOP (such as access to greater capacity and support from other parts of the NCA) and that all NCA officers will receive mandatory training on safeguarding children. The Minister of State for Policing, Criminal Justice and Victims, Damian Green, described becoming an arm of the National Crime Agency as a “game-changer”²⁸ for CEOP because of access to increased resources. Peter Davies told us that incorporation of CEOP into the National Crime Agency was “absolutely a good thing.”²⁹ His predecessor,

21 Q 113

22 *Ibid.*

23 *Ibid.*

24 Q 45

25 Ev 105

26 CEOP Annual Review 2012-2013 & Centre Plan 2013-2014

27 Ev 105

28 Q 204

29 Q 50

Jim Gamble, clearly disagrees. He described subsuming CEOP into the National Crime Agency as “a recipe for disaster”.³⁰ Mr Gamble added:

To take a child protection agency and put it into a national crime agency where the brand has now been diluted, where they will continue to have protection under Freedom of Information, which is fundamentally wrong, how can you have a child protection entity that is not subject to Freedom of Information? You have a child protection entity that is answerable through the NCA to one political person, the Home Secretary. Where is the credible reassurance around that? Where are the lessons of serious case review around professional independence and challenge? The fact of the matter is we had planned the three pillars to be education, social care, and criminal justice. We now have moved to one pillar, which is criminal justice.³¹

17. We recommend that the Government examines whether adequate resources are being deployed to track down online paedophiles in sufficient numbers to act as a meaningful deterrent to others. If not, additional funding should be provided to recruit and train a sufficiently large number of police officers adequate to the task.

18. CEOP has been increasingly effective not least because it is not solely a criminal justice organisation: its education and social care work has also been very important in increasing public understanding of the problem of child abuse and in offering means of countering abusers. We therefore recommend that CEOP continues to publish an annual review which includes an assessment of its ongoing contribution to all three elements of its mission—education, social care and criminal justice.

Surveillance

19. Tracing paedophiles online clearly involves allowing the police to deploy a range of surveillance methods. The Regulation of Investigatory Powers Act 2000 aims to provide a legal regime for both interception of communications and access to communications data that is consistent with human rights legislation—specifically having regard to privacy and proportionality. Peter Davies argued for further changes to the relevant legislation:

It is my firm operational view, and I have articulated it previously, that if there is one piece of legislation that would most help us tackle online child abuse, it would be the provision of a clear, consistent and properly enforced regime for retaining and accessing communications data, because we are regularly in a situation where we are unable to convert, for example, an IP address into a name and address for lack of that precise thing.³²

20. One potential area of operational difficulty was illustrated in evidence from the End Violence Against Women Coalition; their evidence cites CEOP as having warned that live streaming of child abuse through Skype and other platforms is emerging as a growing

30 Q 124

31 Q 119

32 Q 48

method of abusers sharing child abuse images.³³ A government briefing on proposals on the investigation of crime in cyberspace, prepared for the Queen's Speech in 2013, noted:

When communicating over the Internet, people are allocated an Internet Protocol (IP) address. However, these addresses are generally shared between a number of people. In order to know who has actually sent an email or made a Skype call, the police need to know who used a certain IP address at a given point in time. Without this, if a suspect used the internet to communicate instead of making a phone call, it may not be possible for the police to identify them.³⁴

21. A draft Communications Data Bill was announced in the Queen's Speech in 2012 and it was published on 14 June 2012. It was scrutinised by a Joint Committee of both Houses of Parliament and was also considered by the Joint Committee on Human Rights (JCHR) and the Intelligence and Security Committee (ISC). The draft Bill would have extended powers to obtain communications data covering messages sent on social media, webmail, voice calls over the internet and gaming in addition to emails and phone calls. The data could have included the time, duration, originator and recipient of a communication and the location of the device from which it is made. However, it would not have included the actual content of messages. The Joint Committee on the draft Bill published its report on 11 December 2012, concluding that the Bill's scope should be significantly narrowed, while recognising that more needed to be done to provide law enforcement and other agencies with access to data they cannot currently obtain. The Bill would have sat alongside the existing Data Retention (EC Directive) Regulations 2009.³⁵

22. An illustration of both the capability and concerns of internet service providers was given us by Dido Harding of TalkTalk:

I feel very strongly the weight of responsibility as an internet service provider in that our customers place their faith in the fact that it is their data, not our data, to choose what to do with and, therefore, we need a clear legal framework on what we store and what we do not store.

[...]

We do not keep browsing history of where our customers browse every day of the week— that is their data, not ours—unless or until there was a change in legislation that required us to.

[...]

It is very important that the ISPs do not feel like it is a free-for-all to use that data. Our customers do not expect that of us. We have been thinking through, if it is entirely criminal, how we get to a place where we can do that proactively with CEOP.³⁶

33 Ev w85-w88

34 HM Government, The Queen's Speech 2013, 8 May 2013.

35 SI 2009/859

36 Qq 93,95

23. The South West Grid for Learning told us that they have been working with the Internet Watch Foundation and South West police forces since 2006 to flag up any attempted access to websites containing child abuse images (CAI). This pilot project has been managed by CEOP with Home Office approval. Its objective is to flag intelligence to police forces if anyone in a school (specifically) attempts to access a website containing child abuse images. This intelligence prompts the police to then undertake their normal investigation routes and has resulted in a number of school staff being identified and removed as a direct result of what South West Grid for Learning terms a “simple alerting process.”³⁷ They added: “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.”³⁸ **We welcome the increasing use of alerting tools to identify individuals who seek out child abuse and other illegal material online provided these tools are deployed in ways that do not unduly compromise the privacy of the law-abiding majority.**

Internet service providers

24. The scope for further practical action against illegal content is better understood by recognising the different types of providers and how they fit within the current regulatory framework. The Internet Services Providers’ Association identifies four main categories of internet companies:

- Access providers—considered to be “mere conduits” under the e-commerce regulations³⁹ (regulation 17).
- Hosting providers—these include social networks; while these do not have editorial control over content uploaded by users, they may have active or passive moderating policies. Under Regulation 19 of the e-Commerce Regulations they are not liable for the content they host as long as they do not have actual knowledge of unlawful activity or information. “However, upon obtaining such knowledge, hosting providers become liable if they do not act expeditiously to remove or to disable access to the information.”⁴⁰
- Websites where operators have editorial control—content might include a news article and user-generated content like comments on the article.
- Search engines—considered as “caches” under Regulation 18 of the e-Commerce Regulations; search engines “act expeditiously to remove or to disable access to any information if they are made aware of that the fact that this information may be illegal.”⁴¹

37 Ev w49

38 Ev w49

39 The Electronic Commerce (EC Directive) Regulations SI 2002/2013

40 Ev 79

41 Ev 79-80

Internet Watch Foundation

25. The UK internet industry was responsible for founding the Internet Watch Foundation, a membership organisation that serves as the UK hotline where the public can report child sexual abuse content, criminally obscene adult content and non-photographic images of child sexual abuse. In 2012 alone, the IWF processed 39,211 reports and assisted with the removal of 9,696 URLs containing potentially criminal child sexual abuse content. A URL can be as specific as a single image or could refer to an entire website containing potentially thousands of child sexual abuse images or videos. The majority of victims (81%) appeared to be 10 years old or younger (with 4% 2 years old or under) and 53% of the images and videos depicted sexual activity between adults and children, including rape and sexual torture.⁴²

26. When child sexual abuse content is found to be hosted in the UK, the IWF will inform CEOP. After confirmation from CEOP that action can be taken, the IWF will notify the hosting provider who will remove the content from its servers, typically within 60 minutes after receiving the notification from the IWF. This process is commonly referred to as ‘Notice and Takedown’. The IWF can also act against criminally obscene adult content and non-photographic child sexual abuse content hosted in the UK.⁴³

27. When child sexual abuse content is found to be hosted outside the UK (accounting for 99% of known content), the IWF will inform its counterpart hotline in the hosting country through INHOPE, the international association of hotlines, or link in directly with local law enforcement. As other countries take significantly longer to remove child sexual abuse content—50% of the content about which the IWF passes on details internationally is still available after 10 days—the IWF adds the links (URLs) to the content to its URL list (or ‘blocking list’). IWF members can use this list to voluntarily block access to these URLs to protect their customers from stumbling upon the images and videos. The Home Office told us that such blocking arrangements apply to about 98.6% of domestic broadband lines.⁴⁴ Susie Hargreaves of the Internet Watch Foundation told us: “The most effective way to remove content is to remove it at source. It is our view that blocking will only stop inadvertent access and will not stop the determined.”⁴⁵

28. On 18 June 2013, the Secretary of State for Culture, Media and Sport, Maria Miller, hosted a summit on tackling child sexual abuse material on the internet as well as protecting children from harmful or inappropriate content online. Participants included internet service providers, search engines, mobile operators and social media companies. Following the summit, the Secretary of State announced that the Internet Watch Foundation would work with CEOP to actively seek out illegal images of child abuse on the internet. The Internet Watch Foundation told us that, following a donation by Google and additional funding by other members, they will be able to increase their number of

42 Ev 78

43 Ev 77

44 Ev 104

45 Q 34

analysts from 4.5 (FTE⁴⁶) to 11.5 (FTE) and start proactively searching for child sexual abuse content as requested by the Government.⁴⁷

29. We very much welcome the commitment by the Internet Watch Foundation to embark on proactive searching for online child abuse images. The sooner these can be found and removed, the better. However, we are concerned that seven additional staff might prove woefully insufficient to achieve substantial progress towards what must be an important intermediate goal: the eradication of child abuse images from the open internet.

Deterrence

30. The IWF told us that, in addition to “Notice and Takedown” and the URL list, they also compile a keyword list of terms that specifically refer to child sexual abuse content:

This list is used, for instance, by search engines to prevent people from finding images and videos of child sexual abuse content. The keywords are very specific—or very specific combinations of words—that carry no meaning besides the specific reference to child sexual abuse content. This means the keywords will not prevent access to legitimate websites such as, academic research papers into the area of child sexual abuse or websites aimed to help or inform people in relation to child sexual abuse.⁴⁸

31. The Government has asked search engine providers to go further in restricting access to child abuse images. According to the Home Office, they are being asked to develop effective deterrence measures, to ensure child abuse images are not returned in search results, and to prevent any search results being returned “when specific search terms are used that have been identified by CEOP as being unambiguously aimed at accessing illegal child sexual abuse images.”⁴⁹ If progress is not forthcoming, the Government will consider introducing legislation to ensure search engines comply.⁵⁰

32. The IWF is also working with its members to introduce “splash pages”—these are warning messages that appear if a user attempts to access a webpage that has been removed for hosting illegal child abuse images. According to the IWF, “they deliver a hard-hitting deterrence message to users seeking to access child abuse images.”⁵¹ Greater use of splash pages and warning messages “to deter a certain class of person with a low level, opportunist or early interest in child abuse images” is one of a number of tactics put to us by the Children’s Charities’ Coalition on Internet Safety.⁵² Jim Gamble reminded us that splash screens would not result in more hard-core paedophiles being arrested: “it is a diversion of attention and resource that does not work. We tried it.”⁵³ The Home Office pointed out to

46 Full time equivalent

47 Ev 78

48 Ev 77

49 Ev 104

50 Ev 105

51 Ev 104

52 Ev 67

53 Ev 116

us that the objective of further work by search engines and greater use of splash pages “is to make it more difficult for unsophisticated users to find a route from open searching to more sophisticated offending environments, make it more difficult for inquisitive non-offenders to access indecent images of children, and make it less likely that members of the public could inadvertently come across such images.”⁵⁴

33. Search engines and other internet service providers have a vital role in ensuring that access to online child abuse images is prevented and deterred. We expect the Government to monitor closely their degree of commitment and success and to consider the introduction of legislation should they fall short of reasonable expectations.

Other material

34. Much of the evidence we took on illegal content was in relation to child abuse images. However, in the United Kingdom at least, certain categories of extreme adult pornography are illegal both to publish and possess. Pornographic material that explicitly and realistically depicts a variety of non-consensual and injurious practices was outlawed (in England and Wales) by the Criminal Justice and Immigration Act 2008. Similar provisions also appear in the Criminal Justice and Licensing (Scotland) Act 2010, with the notable addition of obscene pornographic images which realistically depict rape or other non-consensual penetrative sexual activity. The Criminal Justice and Courts Bill, currently before Parliament, would extend to England and Wales the definition of the offence of possession of extreme pornographic images to include rape. **We welcome the Government’s decision to include pornographic depictions of rape in the definition of extreme pornography. It has been illegal to publish such images for many years; outlawing their possession is long overdue.**

35. Evidence we received from the Home Office also considered another area within the inquiry’s terms of reference: tackling material intended to promote terrorism or other acts of violence online. A specialist police unit, the Counter Terrorism Referral Unit (CTIRU) proactively seeks and takes down UK-hosted material that breaches the Terrorism Act 2006. UK law has limited application in relation to the significant amount of material hosted overseas; such material “is filtered from parts of the public estate”⁵⁵ (the Government has prioritised schools and some libraries). The filtering can currently be circumvented by users changing their desktop settings; the Government is considering how they can “further restrict access to illegal terrorist material (potentially at the network level), further aligning with the IWF’s approach.”⁵⁶

36. The evidence notes inconsistencies in approach among internet companies. “Whilst engaging with industry to ensure that their own acceptable use policies are being applied rigorously, we are also considering the Home Affairs Select Committee recommendation of establishing a code of conduct for internet companies, distinct from their own terms and

54 Ev 105

55 Ev 106

56 Ev 106

conditions, to improve the response to terrorist material (e.g. including ‘terrorism’ as a category under unacceptable use).”⁵⁷

37. There is clearly a need to obtain wider international consensus and cooperation in relation to combating criminally obscene adult material and terrorist material and we urge the Government to use all the influences it can bring to bear to bring this about within a transparent, legal framework.

3 Adult content

Nature and scale

38. While child abuse images attract worldwide opprobrium, there exists less consensus—both nationally and internationally—on what other kinds of material adults might properly access. Tensions can, and do, arise between the proscription of obscene material and freedom of expression. In the United Kingdom, it is perfectly legal for adults to possess images of explicit sexual activity of a kind that attracts an R18 certificate issued by the British Board of Film Classification. The BBFC told us that their 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.”⁵⁸

39. The BBFC’s written evidence provides a clear reminder of the qualitative difference in the nature and accessibility of pornographic material between the off-line and online worlds:

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.⁵⁹

40. Judging from the evidence we received, pornography was the category of adult content that caused most concern. This could be an indication of its particular prevalence on the internet. The Authority for Television on Demand (ATVOD) told us that five of the top 50 websites most commonly accessed from the UK are “tube” websites offering unrestricted access to hardcore pornography videos. ATVOD also cited figures which suggest that those five sites were (collectively) visited over 214 million times by UK internet users during January 2013.⁶⁰ John Carr of the Children’s Charities’ Coalition on Internet Safety told us that “right now today within the UK, there is nothing there routinely that restricts access to the most bizarre, the most violent and the most graphic types of pornography—anybody can get it.”⁶¹ Pornographic material, much of it illegal, is but “two clicks of a mouse”⁶² away.

58 Ev w14

59 Ev w15

60 Ev w135

61 Q 7

62 Q 7

41. The NSPCC’s Childline service provides one indication of the harm done to young people accessing pornography. According to the NSPCC:

During 2011–12, there were 641 counselling sessions where the young person specifically mentioned being exposed to sexually indecent images. While these incidents will not exclusively relate to online content, a large proportion of this sexually explicit material will have been accessed through internet enabled devices. Young people often told ChildLine that they felt guilty and disgusted about what they had seen and were extremely worried about getting into trouble for accessing these sites. ChildLine has also seen a growing trend of young people talking about being addicted to online pornography.⁶³

42. In January, we held a meeting at the House of Commons with eight young people, some of whom had been harmed by exposure to adult pornography. One young man told us how he had first encountered pornography at the age of eight; viewing pornography had subsequently become a habit which distorted his picture of loving relationships. Another participant told us how, as a teenager, she had been drawn accidentally into viewing pornography from information in a fashion magazine; just one encounter had made her feel ashamed and had affected her relationship with her father. Some girls told us how boyfriends sometimes expected them to behave like “porn stars” and that the exchange of sexually explicit material on mobile phones could lead to bullying.

The law

43. Online activity is subject to general offline legislation such as the Obscene Publications Act 1959 and the Human Rights Act 1998. Publication of obscene material, including child abuse images and extreme adult pornography, is illegal under the Obscene Publications Act 1959 (which extends to England and Wales). An important point is that the definition of obscene depends partly on the person who sees the material. “Legal” adult pornography that has an R18 certificate, issued by the British Board of Film Classification, would likely be classed as obscene if it was published in a way in which children could readily access it. Both the Children’s Charities’ Coalition on Internet Safety and the Authority for Television on Demand (ATVOD) cited case law (in particular, *R v Perrin*) in support of this assertion. The test of obscenity in section 1 of the Act leaves little room for doubt in our minds:

For the purposes of this Act an article shall be deemed to be obscene if its effect or (where the article comprises two or more distinct items) the effect of any one of its items is, if taken as a whole, such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.⁶⁴

44. The internet, where everyone with a connected computer is potentially a publisher, is largely a free-for-all—though some audiovisual content is becoming subject to broadcast-style regulation. The British Board of Film Classification engages extensively with the public in reaching decisions as to what standards are acceptable. The R18 classification is

63 Ev 69

64 Section 1, Obscene Publications Act 1959

given to restricted videos depicting explicit consensual sexual activity which, by definition, excludes so-called “rape porn” and other illegal activities. R18 videos are only allowed to be sold in licensed sex shops (to which only adults are admitted); they may not be supplied by mail order. BBFC certification provides more than a useful yardstick as to content that adults may legitimately choose to access:

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.⁶⁵

45. Transposing accepted standards into the online context represents a challenge for national institutions, not least because the internet is in many ways an international space.

Enforcement

46. Evidence from the Authority for Television on Demand (ATVOD) extensively explores the potential use of the Obscene Publications Act. ATVOD draws attention to the current Crown Prosecution Service guidance for prosecutors on the interpretation of the Obscene Publications Act, which 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 747.⁶⁶

47. ATVOD told us they could find no recent example of a prosecution being launched under the above guidance. John Carr of the Children’s Charities’ Coalition on Internet Safety told us:

That law is being honoured in the breach rather than in the observance. It is principally because most of the publishers are based overseas and the British police have not sought to extradite them or go after them, and that is a great pity. In our evidence, we have made a number of practical suggestions about how we might try to get at least companies that are based in Britain or operate from here to try to observe that particular law. That is to say, “If you are going to publish porn, okay, that is your

65 Ev w15

66 Ev w137

business, but please take concrete steps to make sure kids cannot get easy access to it.”⁶⁷

48. The Parliamentary Under-Secretary of State for Culture, Communications and Creative Industries, Edward Vaizey said: “Obviously nothing should stop us doing the right thing, in terms of prosecutions or clarifying the law. Nevertheless we do have to be aware that a lot of these sites do not provide suitable identification as to who owns them, and again ATVOD is suggesting that we clamp down on those sites by denying them their financial support.”⁶⁸ Jim Gamble did not see access to legal adult pornography primarily as a law enforcement issue. Alluding to the “active choice” filtering solution, he told us: “I will deal with the inappropriate material first because it is the easy one. I think inappropriate material is a parental decision for those individuals who have duty of care of the young people to make and I think active choice is absolutely right. If parents and others are prompted to make a decision, I do not think you can do more than that. You are not going to go out into their homes and look after their children for them.”⁶⁹

49. ATVOD told us that they are working with the UK payments industry to design a process which would enable payments from the UK to be prevented to foreign websites which allow children to view hardcore pornography. However, there needed to be greater clarity over the legality of providing unrestricted access to hardcore pornography.

50. ATVOD has an enforcement role in connection with a limited number of television-like services. It 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, 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. ATVOD’s primary role in relation to protection of minors is founded in Article 12 of the Directive, which forms ATVOD’s Rule 11: “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.”⁷⁰ ATVOD’s evidence anticipates legislation in this area:

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 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.⁷¹

67 Q 6

68 Q 222

69 Q 113

70 Ev w133

71 Ev w135-w136

51. We believe that the existing obscenity laws already proscribe the publication of adult material in ways that make it readily available to children. However, we are concerned that no prosecutions have been brought despite the proliferation of pornography sites which make no attempt to restrict access by children. We welcome the Government's declared intention to legislate to clarify the law in this area. However, in the meantime, we urge the prosecuting authorities to use the existing law to crack down on the worst offenders in order to put pressure on all suppliers of hardcore pornography to make greater efforts to ensure that such material is accessible only by adults.

52. A major difficulty lies in the fact that ATVOD and Ofcom can only regulate services based in the United Kingdom. Furthermore, the requirements of the Audiovisual Media Services Directive are interpreted differently in other Member States. The Dutch regulator, for example, takes the view that hardcore pornography does not seriously impair the development of under 18s and such services operating from the Netherlands are not required to ensure that under 18s cannot normally see or hear them.⁷² In any case, the majority of online hardcore pornography services available to children in the UK operate from outside the European Union (most commonly from the USA).

53. The Government should seek agreement with other European Union Member States to ban on demand programme services that make pornography readily available to children. We further urge the Government to engage with other international partners, particularly the USA, with the aim of securing a similar outcome more widely.

54. Evidence from Ofcom includes a reference to a research report, 'Protecting audiences in a converged world'.⁷³ This research looked at public attitudes within the context of convergence, in order to understand the public's expectations for protection and how content should be regulated in the future: viewers have high expectations of content regulation on broadcast television, and associated video on demand and catch-up services, less so for internet content accessed through devices such as PCs and laptops. Quite how public expectations will develop as smart TVs and other manifestations of media convergence become more commonplace remains to be seen.

55. An independent parliamentary inquiry into online child protection (April 2012), chaired by Claire Perry, suggested that the Government should consider a new regulatory structure for online content, with one regulator given a lead role in the oversight and monitoring of internet content and in improving the dissemination of existing internet safety education materials. Ofcom already has a role in relation to internet services, though this is largely confined to promoting media literacy and performing research. Ofcom told us: "We regulate television channels delivered over the internet and notified ODPS when they are established in the UK; but we have no statutory powers to regulate any other online content."⁷⁴ **We believe that, as part of its existing media literacy duties, Ofcom has an important role in monitoring internet content and advising the public on online safety. However, we are anxious to avoid suggesting a significant extension of formal**

72 Ev w134

73 <http://stakeholders.ofcom.org.uk/binaries/research/tv-research/946687/Protecting-audiences.pdf>

74 Ev 95

content regulation of the internet. Among the unintended consequences this could have would be a stifling of the free flow of ideas that lies at the heart of internet communication.

Age verification

56. Providers of adult content can prevent children from accessing inappropriate and harmful material by putting in place systems that require evidence of age. In this regard, the mobile network operators have stolen a march over the internet service providers. A majority of children have a mobile and an increasing proportion of them go online using a mobile phone or smart phone. The mobile operators' work in online safety is underpinned by a Code of Practice that was first published in January 2004, 'The UK code of practice for the self-regulation of new forms of content on mobile'. The second edition of the code was published in 2009 and the third (and current) edition in July 2013. The Code was the first of its kind and was used as the boiler plate for similar codes introduced by mobile operators throughout the EU.⁷⁵

57. The Code covers a broad range of topics: commercial and internet content, illegal content, malicious communications, spam communications and customer education. A distinction is made between commercial and internet content. The Mobile Broadband Group told us: "The mobile operators' respective responsibilities for commercial content—where they have contractual agreements in place with content providers—as against general content on the Internet are different."⁷⁶ Any commercial content with an 18 rating (determined by the British Board of Film Classification) is placed behind access controls and subject to "a robust age verification process"⁷⁷ (acceptable methods of which are set out in the Code).

58. Age verification is clearly more challenging when accessing content does not involve a direct financial transaction and where the users have an expectation of some degree of anonymity. There is a stark contrast between the requirements on the online gambling industry and those on other providers of online services to adults. As the Remote Gambling Association highlighted:

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.

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

75 Ev 86

76 Ev 86

77 Ev 86

mandatory safeguards in place, but especially where children are concerned we believe that the principles at least should be applied equally.⁷⁸

59. Online gambling of necessity involves a financial transaction which makes age verification relatively easy. There are, however, difficulties in relation to the use of other services or consumption of content which do not necessarily involve direct payment. British Naturism told us: “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.”⁷⁹

60. The Christian social policy charity, CARE, acknowledged 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.”⁸⁰ The Authority for Television on Demand (ATVOD) provided us with further details on the business models of hardcore pornography services, most of which are operated from overseas: “The most frequently accessed services 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).”⁸¹

61. Among the measures recommended by CARE is financial transaction blocking of adult websites that do not put in place “robust” age verification procedures. ATVOD provided us with the following examples of suitable age verification methods:

- Confirmation of credit card 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 age⁸²

78 Ev w7

79 Ev w120

80 Ev w129

81 Ev w134

82 Ev w133

62. The Mobile Broadband Group argues that providers of age restricted services should themselves be putting in place their own processes to protect minors. We agree. **Providers of adult content on the internet should take all reasonable steps to prevent children under 18 from accessing inappropriate and harmful content. Such systems may include, but will not necessarily be restricted to, processes to verify the age of users.**

63. The Children's Charities' Coalition on Internet Safety suggested to us that more could be done in relation to age verification. Their written evidence includes a suggestion that refers to case law supporting the view that publishing adult material in ways that makes it accessible by children is in breach of obscenity legislation: "Nominet should make compliance with *R v Perrin* a condition of operating a .uk domain name e.g. if a site is to publish pornography the operator must give a binding undertaking to put an effective age verification process in place".⁸³ Nominet describes itself as "the trusted guardian of the .uk domain name space, Nominet is responsible for the stability and security of one of the largest internet registries in the world, with more than 10 million registered domain names."⁸⁴ **We have no reason to suppose that Nominet has either the resources or inclination to police the internet. Age verification, while ideal, is not the only way of preventing children from accessing unsuitable content. However, we believe that no .uk site should offer unimpeded access to adult pornography to children. This should be made a condition of registration.**

Site blocking

64. The site blocking approach enabled by the Internet Watch Foundation, with the necessary cooperation of ISPs, is one instrument—albeit a blunt one—aimed at preventing access (by anyone) to online material. It has so far been applied mainly to images of child abuse. Extending this approach to other material, including some adult sites, would face challenges both of scale and cost. BCS⁸⁵, the Chartered Institute for IT, told us:

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.

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.⁸⁶

65. BT, a major ISP, has also expressed concerns:

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

83 Ev 65-66

84 www.nominet.org.uk/uk-domain-names

85 Formerly known as the British Computer Society

86 Ev w35

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.

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.⁸⁷

66. The Internet Watch Foundation describes blocking of child abuse sites as “a short-term disruption tactic which can help protect internet users from stumbling across these images, whilst processes to have them removed are instigated.”⁸⁸ **Site blocking is highly unlikely to be a suitable approach for adult pornography or violent material much of which is legal (at least if it is unavailable to minors) and which is prevalent on the internet. However, blocking should be considered as a last resort for particularly harmful adult websites that make no serious attempt to hinder access by children.**

Filters

67. An independent parliamentary inquiry into online child protection (April 2012), chaired by Claire Perry, noted that “while parents *should* be responsible for monitoring their children’s internet safety, in practice this is not happening”.⁸⁹ The report went on to recommend that the Government “should launch a formal consultation on the introduction of an Opt-In content filtering system for all internet accounts in the UK” as well as seeking “backstop legal powers to intervene should the ISPs fail to implement an appropriate solution”.⁹⁰ Following a subsequent Department for Education consultation, the Government stopped short of proposing a default-on or opt-in filtering system, partly on the grounds of practicality, the danger of blocking legitimate sites and the inability of such systems to cut off other types of harmful material such as grooming and bullying. The Perry report came on the back of a number of other studies that have looked at how best to protect children, for example, Reg Bailey’s *Letting Children be Children* (June 2011) and Tanya Byron’s *Safer children in a digital world* (March 2008). The latter report led to the setting up of the UK Council on Child Internet Safety in September 2008. Our predecessor Committee also published its report, *Harmful content on the Internet and in video games*, in July 2008.

68. In its evidence, the Department for Culture, Media and Sport notes that 91% of children live in households with internet access and that a greater proportion of children aged 12–15 own smartphones than adults. The Government “understands that, first and

87 Ev w57-w58

88 www.iwf.org.uk/members/member-policies/url-list

89 *Independent parliamentary inquiry into online child protection: findings and recommendations*, April 2012, p5

90 Ibid, p8

foremost, responsibility for keeping children safe online falls to parents and guardians; however, Government is acting to ensure that parents have the tools and information they need to be able to do so.”⁹¹ In particular, the Government has been working through the UK Council for Child Internet Safety (UKCCIS) “to pursue a voluntary approach to child internet safety and has called on industry to make the right tools available to allow parents to protect children online.”⁹²

69. In their submission, Intellect rehearsed the roles the technology industries have been playing in the development of parental control tools such as filters. They also refer to a “continual process to innovate and update these tools”.⁹³ Intellect added:

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.⁹⁴

70. In a speech to the NSPCC on 22 July 2013,⁹⁵ the Prime Minister announced a range of measures to tackle the “corroding” impact of online pornography on childhood. Some of these would prevent children from being able to access (legal) pornography while other measures would target child abuse images and the activities of paedophiles.

71. On access to pornography, Mr Cameron said that by the end of the year, family-friendly filters would automatically be selected for all new broadband customers (unless the account holder chose otherwise). Once installed, the filters would cover any device connected to the customer’s internet account and only the account holder, who must be an adult, would be able to change the filters. Internet service providers would be given until the end of 2014 to contact existing customers and present them with an “unavoidable decision” about whether or not to install family friendly content filters.

72. In March 2012, TalkTalk had become the first internet service provider to introduce a genuine “unavoidable choice” for new customers when they signed up to TalkTalk broadband, as per the recommendation of the Bailey Review. TalkTalk told us that customers are asked to make a ‘yes’ or ‘no’ decision as to whether they want to filter access to content that might be inappropriate for under 18s on their broadband connection or not.⁹⁶ TalkTalk then applies this to their internet connection as soon as it is live, and no further action is required by the customer. The customer is also alerted by email and/or text if any of the so-called Homesafe settings are changed – safeguards such as this aim to ensure children aren’t changing settings without their parents’ knowledge.

91 Ev 108

92 Ev 108

93 Ev w140

94 *Ibid.*

95 <https://www.gov.uk/government/speeches/the-internet-and-pornography-prime-minister-calls-for-action>

96 Ev 83

73. The Internet Service Providers' Association told us: "The main consumer facing ISPs are moving to a system where new and existing customers are presented with an unavoidable choice of whether to apply filters or not. These filters cover the whole home ... Some smaller consumer-facing providers are considering solutions that offer family friendly filters but can be deployed on smaller scale and at lower costs. ISPA is currently discussing this issue with its members."⁹⁷ Claire Perry told us that the top four ISPs are introducing "unavoidable choice" filtering solutions. She said: "we would like the others to commit to the same thing. They will ask you in different ways. Some might ask you when you go to query your bill online, some may interrupt your browsing session, which is a first for the UK to do that. This is the commitment that Ofcom will be monitoring. Every household will be contacted and asked whether or not they would like to switch on the filters, and the box, "Yes, please" will be pre-ticked."⁹⁸

74. We welcome the introduction of whole home filtering solutions that prompt account holders with a choice to apply them. We encourage all internet service providers to offer their customers this valuable service. Ofcom should monitor the implementation of this filtering and report back on its level of success and adoption.

75. While greater use of filters is welcome, they should not be seen as a panacea. ATVOD told us: "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."⁹⁹ ATVOD further cites EU Commission research which 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). Although the efficacy of parental controls may have improved since that research was conducted in 2011, ATVOD told us it is clear that both "over-blocking" and "under-blocking" still occur.¹⁰⁰ The Internet Service Providers' Association told us that filtering does have limitations and that over-blocking and under-blocking of content "is inevitable".¹⁰¹

76. When we held a meeting with eight young people in January, we heard varying views on filtering. Some called for stronger filtering to prevent access to harmful material online, particularly pornography. We were told of boys circumventing the filters in place in school to access age-inappropriate content. However, others expressed concern that if filters were too strong or inappropriately applied, young people could be prevented from accessing websites offering advice on sexual health and online safety.

77. TalkTalk described its 'Homesafe' system as a "whole home parental controls system that allows parents to protect every device connected to the home broadband and control the types of websites their family is able to visit."¹⁰² Homesafe has three features:

97 Ev 80

98 Q 207

99 Ev w137

100 Ev w138

101 Ev 81

102 Ev 82

- Kids Safe—parental controls that allow the account holder to block content they don't want to be accessed on their connection. There are nine different categories, and customers can also choose to block other specific websites.
- Virus Alerts—an alert system that blocks access to web pages infected with malware¹⁰³ and phishing sites.¹⁰⁴
- Homework Time—this allows parents to block social networking and online games sites—common sources of distraction for children from homework—during a specified time of day.

The Association for UK Interactive Entertainment describes as “deeply troubling” the inclusion of games in the TalkTalk list. They told us of the “potential for this to do significant collateral damage to the UK games industry.”¹⁰⁵ **We value the UK games industry and the many educational and recreational benefits it provides to children. As filtering technologies continue to develop, as they should, we trust parents will be empowered to provide the supervision they want of what games their children play and when.**

78. In connection with filters applied by mobile network operators, the BBFC has a role in calibration: providing advice to mobile operators on where to set their Internet filters. The Mobile Broadband Group told us that processes also exist to remedy inadvertent or unfounded over-blocking. The Group also told us: “The BBFC framework is binary—18 or unrestricted. This is because 18 is the only age at which it is currently practical to implement convenient, ubiquitous and robust on-line age verification. Stricter filters are available in the market for parents that may want a narrower range of content for younger users but these fall outside the Code.”¹⁰⁶ At a recent seminar, Adam Kinsley, Director of Policy, BSkyB, gave details of that ISP's more granular filtering solution which has additional age categories analogous to those used for cinema exhibition.¹⁰⁷

79. The Mobile Broadband Group reminded us that mobile operators have had network filtering in place for nearly ten years. They added: “Great pressure has also recently been put on the domestic ISPs and public wi-fi operators to do the same—and this is happening. However, all these efforts would be complemented with the availability of better user controls at operating system and device level. The UK, through UKCCIS and other channels, should continue to examine closely what the manufacturers and operating system providers are offering in the area of child safety and challenge them to be as equally committed as the network providers.”¹⁰⁸ **We agree that the availability and performance of filtering solutions must be closely monitored, both for efficacy and the avoidance of over-blocking. It should also be easy for websites inadvertently blocked to report the fact and for corrective action to be taken.**

103 Malicious software

104 Phishing sites aim to obtain personal data by deception

105 Ev w92

106 Ev 87

107 Westminster eForum Keynote Seminar, Childhood and the internet – safety, education and regulation, 29 January 2014

108 Ev 88

80. A recent report by Ofcom notes: “The provision of accurate content labels or metadata by content providers would help filtering systems to categorise content correctly. However, only a tiny proportion of websites are labelled in a way that allows easy categorisation for the purposes of filtering.”¹⁰⁹ **Websites that provide adult content should signal the fact clearly to enable filters better to take effect. A failure on the part of the operators of such sites to do so should be a factor in determining what measures should be taken against them.**

81. One of the arguments given against filtering is the ease with which it can be circumvented. According to Ofcom research, most parents report that they know enough to keep their child safe online, but around half of parents continue to feel that their child knows more about the internet than they do, including 14% of parents of children aged 3–4. Ofcom also acknowledges: “In some cases, children will be able to bypass filters, either by altering the filtering settings or by using tools to conceal the sites they are visiting from the filtering software. The main mechanisms by which filters may be bypassed are through the use of a VPN (virtual private network), which encrypts all internet traffic, and the use of proxy sites.”¹¹⁰ Ofcom research has also established that 18% of children aged 12–15 know how to disable online filters or controls, but considerably fewer (6%) have done this in the past year. **Filters are clearly a useful tool to protect children online. Ofcom should continue to monitor their effectiveness and the degree to which they can be circumvented.**

Media literacy and education

82. Filtering systems will in general fail to capture text and picture messages sent directly between individuals. Andy Phippen, Professor of Social Responsibility in Information Technology, Plymouth University, told us about some of the discussions he has had with young people themselves:

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.¹¹¹

83. Comments such as this serve only to highlight the importance of media literacy and education. The difficulty in entirely preventing access to age-inappropriate material emphasises the importance of e-safety in the school curriculum and the availability of advice to parents and carers. Such advice should include how to report harmful material. Evidence we received from the DCMS did highlight the role of education in online

109 Ofcom Report on Internet safety measures: Strategies of parental protection for children online, 15 January 2014

110 *Ibid.*

111 Ev w111

safety.¹¹² From September 2014, the national curriculum will extend e-safety teaching to pupils aged between 5 and 10 (11-16 years olds are already covered). The DCMS also referred to several general educational tools and programmes: Think U Know (from CEOP); the UK's Safer Internet Centre (which has a hotline for internet safety information); Get Safe Online (providing advice at the initiative of government, law enforcement, businesses and the public sector); online resources, including Know IT All, from the Childnet charity; the South West Grid for Learning and ParentPort. The last of these is a complaints portal that directs individuals to the relevant media regulator, or to sources of advice for content that has no regulator responsible. Edward Vaizey told us: "Ofcom was behind setting up ParentPort because it felt you needed a one-stop shop for parents to go to get all the advice they needed."¹¹³ **We welcome the introduction of ParentPort but believe Ofcom should seek to promote and improve it further. For example, more use could be made of it to collect data on complaints concerning children's access to adult material.**

84. We further recommend that Ofcom regularly reports on children's access to age-restricted material, particularly adult pornography and the effectiveness of filters and age verification measures. Ofcom is well-placed to fulfil this role given the work it does on its Children and Parents: Media Use and Attitudes Report.

85. Childnet International commented on the need for further work on the education front:

There is a need for ongoing educational and awareness work in this area ... 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.

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.¹¹⁴

Safer Internet Day 2014 was subsequently celebrated by 106 countries, and early indications are that it was a great success: over 25 million people were reached by the "SID2014" Twitter hashtag alone.¹¹⁵

86. In their evidence, the sexual health charities FPA¹¹⁶ and Brook included the following: "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

112 Ev 109

113 Q 206

114 Ev w90

115 <https://infogr.am/sid-2014-overview?src=web>

116 Family Planning Association

guidance for the modern era.”¹¹⁷ The young people we met in January were unanimous that schools should be required to offer sex and relationships education. As one young person put it, teachers are a sounder source of professional information on sex than friends or the internet. The young people said providing them with the knowledge, tools and confidence to navigate potential online dangers would ultimately be more beneficial than technical measures. The NSPCC recently told us that the Government has committed to emailing every school SRE advice developed by Brook, the sex education forum, and others.¹¹⁸ **We note comments on the state of, and access to, sex and relationships education. We are aware this is a politically contested subject but believe the Government should take into account the views of the young people who gave evidence to us of the value and importance of good quality mandatory sex and relationship education as policy develops. In the mean time, teachers have many opportunities to use their professional judgement in advising children both on online safety and on respect for each other. We believe there is scope for providing teachers with clearer signposting of the advice and educational resources that are already available.**

117 Ev w100

118 Ev 112

4 Social media

Nature and scale

87. From chat rooms to Facebook, from Snapchat to Twitter, social media platforms play to the human desire to keep in touch. Online social media provide new ways of interacting and for modified ways of behaving. Everyone with a connected computer is now a potential publisher and some people publish with too little regard for the consequences—for others as well as themselves.

88. The most recent research¹¹⁹ from the NSPCC shows that 28% of young people who have a social networking profile have experienced something that has upset them in the last year. These experiences include cyber-stalking, being subjected to aggressive or offensive language, being sent sexually explicit pictures and being asked to provide personal or private information. However, the greatest proportion of the group (37%) had experienced “trolling”.¹²⁰ Alongside this evidence that online bullying is clearly a problem for young people, the latest Childline statistics show an 87% increase in 2012/13 in the number of young people contacting the NSPCC for support and advice about being bullied via social networking sites, chat rooms, online gaming sites, or via their mobile phones. The NSPCC attributes this trend in part to the increasing ownership by young people of smartphones and tablets.

89. The results of a July 2013 survey by the bullying prevention charity, BeatBullying, provide further evidence of both the nature and scale of online bullying and the dangerous sides of the internet:

- One in five 12–16 year-olds have interacted with strangers online
- More than a third of 12–16 year-olds go online most often in their own bedroom
- One in five 12–16 year-olds think being bullied online is part of life
- More than a quarter of 12–16 year-olds admitted to witnessing bullying online, but only half of these did something about it
- The primary reasons young people gave for not doing anything about the online bullying was being worried about being bullied themselves or not knowing who to speak to about it
- Almost a quarter (23%) of 12–16 year-olds spend more than five hours a day online during school holidays; more than double the number during term time (10%)
- The majority (80%) of 12–16 year-olds said they feel safe online, compared to only 60% of the younger age group (8–11 year-olds). But worryingly, one in five (22%) of 12–16 year-olds said they think being bullied online is part of life

119 Ev 111

120 Trolling: the practice of posting deliberately inflammatory material.

- For those 12–16 year-olds who did do something about the cyber bullying, most went to their parents for advice; however, only 38% of parents think their children are at risk of being bullied online.¹²¹

90. Anthony Smythe of BeatBullying told us: “Our research would suggest that one in three children have experienced cyber-bullying. More worrying is that you will find that one in 13 are subject to persistent cyber-bullying and that is what leads to the cases of suicide and self-harm that we have seen over the recent summer months.”¹²² Our own conversations with young people left us in little doubt as to the corrosive effect of bullying—often perpetrated by “friends”.

91. Two of the best known social media platforms (there are many) provided both written and oral evidence in the course of our inquiry: Facebook and Twitter. Written evidence from Facebook begins by describing its mission “to make the world more open and connected and to give people the power to share.”¹²³ Facebook is a global community of more than 1.15 billion people and hundreds of thousands of organisations. Facebook works “to foster a safe and open environment where everyone can freely discuss issues and express their views, while respecting the rights of others.”¹²⁴

92. Twitter told us of their 200 million active users across the world and 15 million in the UK alone; the platform now serves 500 million tweets a day. “Like most technology companies we are clear that there is no single silver bullet for online safety, rather it must be a combined approach from technology companies, educators, governments and parents to ensure that we equip people with the digital skills they will need to navigate the web and wider world going forward.”¹²⁵

The law

93. Evidence from the DCMS makes the general point that behaviour that is illegal off-line is also illegal online.¹²⁶ Communications sent via social media are capable of amounting to criminal offences in relation to a range of legislation, including:

- Communications which may constitute credible threats of violence to the person or damage to property.
- Communications which specifically target an individual or individuals and which may constitute harassment or stalking within the meaning of the Protection from Harassment Act 1997.
- Communications which may be considered grossly offensive, indecent, obscene or false.¹²⁷

121 Ev 75

122 Q 5

123 Ev 89

124 Ev 89

125 Ev 92

126 Ev 109

94. The Director for Public Prosecutions published guidelines for prosecutors when considering cases involving communications via social media. Relevant legislation includes: Malicious Communications Act 1988; section 127, Communications Act 2003; Offences Against the Person Act 1861; Computer Misuse Act 1990; Protection from Harassment Act 1997; Criminal Justice and Public Order Act 1994; section 15, Sexual Offences Act 2003 (for grooming).

95. The DCMS cites data from the Crime Survey of England and Wales which shows that, in 2011/12, 3.5% of adults (aged 16 and over) had experienced upsetting or illegal images. 1.4% had experienced abusive or threatening behaviour. Some of these experiences are likely not to have met the criminal threshold.¹²⁸

96. BeatBullying have argued for greater clarity in the law; they told us:

More than 1,700 cases involving abusive messages sent online or via text message reached English and Welsh courts in 2012. However, cyberbullying is not a specific criminal offence in the UK. Some types of harassing or threatening behaviour—or communications—could be a criminal offence. These laws were introduced many years before Twitter, Facebook and Ask.FM, and they have failed to keep pace with the demands of modern technology. Unfortunately, serious cases of cyberbullying, which have often resulted in suicide, have dominated our headlines in recent months. That is why BeatBullying have been calling on the Government to review current legislation and make bullying and cyberbullying a criminal offence so that children and young people have the protection they need and deserve, at the earliest opportunity, to avoid this escalation.¹²⁹

97. BeatBullying's evidence went on to cite the recent Anti-Social Behaviour, Crime and Policing Bill as a possible vehicle for introducing bullying and cyberbullying as a form of anti-social behaviour. Jim Gamble told us: "The Prevention of Harassment Act is bullying. The Prevention of Harassment Act is trolling ... We need to ensure that the laws as they exist, when they can be applied, are applied."¹³⁰ **Any changes to legislation, including consolidation of current laws, which clarify the status of bullying, whether off-line or online, would be welcome. At the same time, much could be achieved by the timely introduction of improved guidance on the interpretation of existing laws.**

Enforcement

98. On Twitter, users "agree" to obey local laws. Twitter's rules and terms of service "clearly state that the Twitter service may not be used for any unlawful purposes or in furtherance of illegal activities. International users agree to comply with all local laws regarding online conduct and acceptable content."¹³¹ A question that arises is how more could be done by Twitter and other social media providers to assist in compliance with the law.

127 Ev 109-110

128 Ev 110

129 Ev 76

130 Q 116

131 Ev 92

99. Facebook's detailed Statement of Rights and Responsibilities ("SRR") describes the content and behaviour that is and is not permitted on its service. With respect to safety, the SRR specifically prohibits the following types of behaviours:

- Bullying, intimidating, or harassing any user.
- Posting content that: is hate speech, threatening, or pornographic; incites violence; or contains nudity or graphic or gratuitous violence.
- Using Facebook to do anything unlawful, misleading, malicious, or discriminatory.¹³²

100. Both Facebook and Twitter have sensible terms and conditions attaching to the use of their services. However, these should be made much clearer, explicit and visible. People who might be tempted to misuse social media need to be left in no doubt that abuses online are just as unacceptable as similar misbehaviour face-to-face.

101. Facebook encourages people to report content that they believe violates their terms. "Report" buttons are "on every piece of content on our site." "When we receive a report, we have a dedicated team of professionals that investigate the piece of content in question. If the content in question is found to violate our terms, we remove it. If it does not violate our terms, then we do not remove it. We also take action, such as disabling entire accounts (eg of trolls) or unpublishing Pages, if deemed necessary."¹³³ Reports are handled by the User Operations team comprising hundreds of employees located in India, Ireland and the USA. The User Operations team is separated into four specific teams covering safety, hate and harassment, access and abusive content.

102. Facebook is aware that many under-13s are falsifying their ages to open accounts, in violation of the Statement of Rights and Responsibilities. Often parents assist them in doing so, something that Facebook's Simon Milner has reportedly¹³⁴ likened to allowing younger children to view Harry Potter video works (some of which have a '12' certificate). Sinéad McSweeney of Twitter told us: "We do not collect age information on sign-up. I think Twitter has established a reputation in the area of privacy. We minimise the amount of information that we require from users to sign up so we do not collect age or gender or other details about our users. Where it comes to our attention that somebody under the age of 13 is using the platform, their accounts are removed."¹³⁵ She went on to imply that a child under 13 would either have to be aware of this age rule, or read about it in Twitter's privacy policy.¹³⁶

103. Claire Lilley of the NSPCC suggested: "Some of these sites need more human moderators to look for the fake accounts. That is one part of it, but they also have very sophisticated algorithms where they look at what language people are using, what sites they are visiting and what they are talking about online. They can tell with quite a degree of

132 Ev 89

133 Ev 89

134 [Facebook admits it is powerless to stop young users setting up profiles](#), *Guardian*, 23 January 2013

135 Q 166

136 Q 169

sophistication a lot about the individuals. Twitter, for example, has a minimum age of 13, but when you sign up to Twitter, you do not have to put in your date of birth. There is nothing to stop you. Twitter would say that what it does is to look at its algorithms to spot the children who are under 13 and therefore potentially on a site that is aimed at an older audience and containing information, posts and so on that are not suitable for their age. Its argument is that it uses very sophisticated algorithms, so I think there is a lot more that the sites could do.”¹³⁷

104. Twitter’s age-verification process could at best be described as algorithmic and reactive; non-existent might be a more accurate description. **Given that Facebook and Twitter are aware of the extent to which their services are accessed by younger children, we expect them to pay greater attention to factoring this into the services provided, the content allowed and the access to both. The same applies to other social media companies in a similar position.**

105. BeatBullying told us that BeatBullying.org is the only e-mentoring and social networking site to be endorsed by CEOP. “We strongly believe that our approach to online safety must be adopted by all internet providers if children and young people are to be safe online.”¹³⁸ This website checks all content prior to it being uploaded. As a general policy, Twitter told us that they do not mediate content. However, there are some limitations on the type of content that can be published with Twitter. These limitations include prohibitions on the posting of other people’s private or confidential information, impersonation of others in a manner that does or is intended to mislead, confuse, or deceive others, the posting of direct, specific threats of violence against others, and trademark and copyright infringement.¹³⁹ **Twitter told us that users can mark their own tweets as sensitive which by default means a warning message is posted to anyone wishing to view these. This is a good reminder that self-restraint and self-regulation are crucial aspects of any enforcement regime in the online world.**

106. **In spite of reassuring words from Facebook and Twitter, it is clear that these platforms, in common with other social media providers, could do far more to signal the unacceptability of abuse and to stamp it out when it arises.**

107. Offensive communications via social media that do not cross the threshold into criminal behaviour should, the Government expects, be dealt with expeditiously by the social media companies.¹⁴⁰ We agree. **Social media providers should follow the examples of Facebook and Twitter in having appropriate terms and conditions. We believe there is significant scope for such providers—including Facebook and Twitter—to enforce such conditions with greater robustness.**

137 Q 22

138 Ev 73

139 Ev 92

140 Ev 111

Reporting

108. A service for reporting all hate crimes online was launched by the police in April 2011. The website, called True Vision, is supported by all forces in England, Wales and Northern Ireland and can be accessed at www.report-it.org.uk. All reports of incitement to racial hatred content hosted in the UK previously reported to the Internet Watch Foundation (IWF) should now be reported directly to True Vision. True Vision takes reports about: racist or religious hate crime; homophobic and transphobic hate crime; disability hate crime; bullying and harassment; domestic abuse. The National Centre for Cyberstalking Research commented: “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.”¹⁴¹

109. Social media providers generally offer reporting mechanisms, with varying degrees of user-friendliness and degree of follow-up. In serious cases, the access providers will also get involved. TalkTalk told us that they investigate any abusive or threatening comments posted on sites by their customers when provided with the log information that supports the complaint. In severe cases, relevant data will be disclosed to the third party solicitor, on receipt of a fully sealed court order from a UK court.¹⁴²

110. As noted above, Facebook told us about their ‘report’ buttons. Twitter also told us that they have now introduced a similar reporting facility. Twitter said that reports that are flagged for threats, harassment or self-harm are reviewed manually. Twitter advises users to report illegal content, such as threats, to local law enforcement and refers to working closely with the police in the UK.¹⁴³ Stella Creasy MP—who has herself been subject to bullying and threats via social media—argued for the introduction of an “online panic button system” to alert sites like Twitter to an emerging problem.¹⁴⁴ She told us how she had been subjected to graphic threats and harassment on Twitter over the course of two weeks.¹⁴⁵ Even this was “just a fraction” of what had been endured by Caroline Criado-Perez who had been receiving 50 rape threats an hour. These threats evidently started for no reason other than Ms Criado-Perez’s successful campaign to keep female representation on English bank notes. In January, two people were jailed for their roles in the abuse to which Caroline Criado-Perez was subjected.¹⁴⁶ Another individual has recently been charged with sending malicious communications to Stella Creasy MP.¹⁴⁷ All were charged under section 127 of the Communications Act 2003.

111. The NSPCC have suggested that providers of social media services should provide a range of options for users to report material, with extra support for younger users. They add that default privacy settings should be the highest possible and there should be

141 Ev w144

142 Ev 85

143 Ev 93

144 Q 70

145 Q 61

146 “Two jailed for Twitter abuse of feminist campaigner”, *Guardian*, 24 January 2014

147 “Man charged over MP Stella Creasy tweets”, BBC News, 23 January 2014

adequate use of human moderators.¹⁴⁸ Claire Lilley of the NSPCC told us that, even if children report bullying to social networking sites, “they often feel like nothing is being done as a result of that and that no action is being taken, so children, when it is happening to them, [are] feeling extreme vulnerability and humiliation, and a sense of helplessness.”¹⁴⁹ These comments were borne out by one of the teenage girls we talked to in January who told us that, with Facebook, it was hard to get bullying material taken down or blocked; when it was eventually removed, the damage had already been done. Twitter continues to be criticised for not doing enough to combat abusive and threatening behaviour online,¹⁵⁰ even in the wake of the limited and tardy corrective action it took following last year’s case involving Caroline Criado-Perez and Stella Creasy MP.¹⁵¹

112. Anthony Smythe of BeatBullying said:

I would like more transparency of the websites to hear from the big websites about how many cases of cyber-bullying are reported to them each year. What did they do about them? How quickly did they respond to those cases? What support and help did they offer? It is about having a bit more accountability. They will say that they probably do that, and if you spend five hours on the internet, you might find that information annexed somewhere. I would like that information signposted on their main websites so that parents and young people can have access and understand the website that they are using.¹⁵²

113. Stella Creasy MP told us: “One of the other things I have asked the companies to do is publish their data about the numbers of reports of abuse they get and the numbers of the concerns so we can get a question of scale.”¹⁵³

114. Social media providers should offer a range of prominently displayed options for, and routes to, reporting harmful content and communications. They need to act on these reports much more quickly and effectively, keeping the complainant and—where appropriate—the subject of the complaints informed of outcomes and actions.

115. Ofcom should monitor and report on complaints it receives, perhaps via an improved ParentPort, regarding the speed and effectiveness of response to complaints by different social media providers.

Advice and support

116. Anthony Smythe of BeatBullying told us: “What is the greatest concern for children and young people—and now for adults—is the feeling that they are helpless and are

148 Ev 73

149 Q 10

150 “Ex-footballer Collymore accuses Twitter over abusive messages”, BBC News, 22 January 2014

151 Q 61

152 Q 14

153 Q 66

hopeless in terms of getting advice and support. They do not know where to go to.”¹⁵⁴ BeatBullying develops these points in their written evidence:

Everyone involved with children’s and young people’s use of the internet—parents, schools, service providers, organisations and children themselves—has a shared responsibility for online safety. That is why in April 2013 BeatBullying launched a campaign for better anti-bullying protections called Ayden’s Law. The campaign calls for a national strategy to tackle cyberbullying and would set out how the voluntary and community sector, parents and schools would be equipped to (a) protect the children in their care from harm online and (b) educate and equip children about internet safety and responsible digital citizenship so that they understand the issues for themselves.

Any approach to online safety must ultimately be about shaping attitudes and changing behaviors as much as it is about teaching techniques for staying safe or for anything else.¹⁵⁵

117. Claire Lilley said: “I would say that what bullying on social media comes down to is about behaviour. We can wave the long arm of the law at children, but what we need to do is to educate them about the impact of the behaviour in which they are engaging on people who are at the receiving end of it. We need to do much more to educate them to build their resilience, both when they are on the receiving end, but also to build their empathy and their sense of respect for other children.”¹⁵⁶

118. The Home Office told us that they undertake to “work with DCMS to ensure we are linked into initiatives such as Safer Internet Centre and Get Safe Online, which provide internet safety information and advice alongside a wealth of internet safety resources for schools and information for parents and children.”¹⁵⁷

119. Social media companies could, and in some cases do, provide resources and funding for educational initiatives. For example, Simon Milner of Facebook, referred to support given to the South West Grid for Learning which is “particularly helpful”¹⁵⁸ for schools and teachers. He also indicated that a request for funds would be listened to “with a very open mind.”¹⁵⁹ We also heard evidence from the Government, Facebook and Twitter of the value of the helpline operated by the UK Safer Internet Centre, which operates on minimum and time-limited funding from the European Union. **We believe it is in the interests of social media platforms, if they wish to avoid a more regulatory approach, to put their money where their mouths are and provide more funding for the valuable work being done on internet safety by voluntary organisations and charities.**

154 Q 5

155 Ev 73

156 Q 12

157 Ev 107

158 Q 138

159 Q 150

120. A good deal of advice on the safe use of social media is available already. This should be signposted more clearly for teachers, who are likely to be in the front line when it comes to dealing with bullying both in the playground and in the online world.

Anonymity

121. The cloak of anonymity is a useful one for a dissident or free-thinker to wear; but it can also mask the bully and the criminal. Evidence from Dr Claire Hardaker, a Lecturer in Corpus Linguistics, identifies anonymity as one of the factors that can lead to harmful behaviour online (others include detachment and entertainment). She notes: “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.”¹⁶⁰ She goes on to question the feasibility of removing anonymity:

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.¹⁶¹

122. These views appear at odds with those of John Carr of the Children’s Charities’ Coalition on Internet Safety. Referring to the “abuse of anonymity” he emphasised the importance of being able to trace individuals; this would require social media providers to take greater steps to verify the identity of their account holders.¹⁶² He said: “So the requirement on internet service providers would be to verify that the individual who has just signed up with them is not in fact a dog, but an actual human being with an actual and verified address where they can be reached. That alone would act as a major brake on a lot of the bad behaviour.”¹⁶³

123. The Open Rights Group told us: “It is too easy to assume that tackling anonymity online is a simple solution to abusiveness.” The Group added:

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.¹⁶⁴

160 Ev w2

161 Ev w4

162 Qq 22-26

163 Q 24

164 Ev w126

124. Nicholas Lansman of the ISPA said: “People can attempt to hide themselves online, but there are technical ways in which they can be discovered.”¹⁶⁵ Claire Perry MP referred to a particularly tragic case when she told us: “I was encouraged with Ask.fm—having spent a lot of time with Hanna Smith’s father, who was one of the young women who did indeed commit suicide—that company did set up a facility where users could choose to be anonymous, but you would know if the user was anonymous when you were exchanging information with them.”¹⁶⁶

125. Anonymity is not just a cloak for cowards who bully; it is used by others to disguise their criminal activities. In January of this year, the National Crime Agency announced that 17 Britons had already been arrested as a result of Operation Endeavour, spanning 14 countries. This particular case involved the live streaming of child abuse in the Philippines for viewing across the world. The prevalence of child abuse images on the internet and the associated activities of paedophiles provide just one of the starkest of reminders that keeping children safe off-line includes keeping them safe online too.

Conclusions and recommendations

1. We believe that the Government should, in due course, consolidate the law around child abuse images into a single Act of Parliament with a view to providing even greater clarity for the purposes of law enforcement and deterrence. (Paragraph 9)
2. Given the worldwide nature of online crime, we recommend that the Government press for wider international adoption of both the Budapest and Lanzarote Conventions. The Government should ratify the Lanzarote Convention as soon as practicable. (Paragraph 10)
3. We recommend that the Government examines whether adequate resources are being deployed to track down online paedophiles in sufficient numbers to act as a meaningful deterrent to others. If not, additional funding should be provided to recruit and train a sufficiently large number of police officers adequate to the task. (Paragraph 17)
4. CEOP has been increasingly effective not least because it is not solely a criminal justice organisation: its education and social care work has also been very important in increasing public understanding of the problem of child abuse and in offering means of countering abusers. We therefore recommend that CEOP continues to publish an annual review which includes an assessment of its ongoing contribution to all three elements of its mission—education, social care and criminal justice. (Paragraph 18)
5. We welcome the increasing use of alerting tools to identify individuals who seek out child abuse and other illegal material online provided these tools are deployed in ways that do not unduly compromise the privacy of the law-abiding majority. (Paragraph 23)
6. We very much welcome the commitment by the Internet Watch Foundation to embark on proactive searching for online child abuse images. The sooner these can be found and removed, the better. However, we are concerned that seven additional staff might prove woefully insufficient to achieve substantial progress towards what must be an important intermediate goal: the eradication of child abuse images from the open internet. (Paragraph 29)
7. Search engines and other internet service providers have a vital role in ensuring that access to online child abuse images is prevented and deterred. We expect the Government to monitor closely their degree of commitment and success and to consider the introduction of legislation should they fall short of reasonable expectations. (Paragraph 33)
8. We welcome the Government's decision to include pornographic depictions of rape in the definition of extreme pornography. It has been illegal to publish such images for many years; outlawing their possession is long overdue. (Paragraph 34)
9. There is clearly a need to obtain wider international consensus and cooperation in relation to combating criminally obscene adult material and terrorist material and

we urge the Government to use all the influences it can bring to bear to bring this about within a transparent, legal framework. (Paragraph 37)

10. We believe that the existing obscenity laws already proscribe the publication of adult material in ways that make it readily available to children. However, we are concerned that no prosecutions have been brought despite the proliferation of pornography sites which make no attempt to restrict access by children. We welcome the Government's declared intention to legislate to clarify the law in this area. However, in the meantime, we urge the prosecuting authorities to use the existing law to crack down on the worst offenders in order to put pressure on all suppliers of hardcore pornography to make greater efforts to ensure that such material is accessible only by adults. (Paragraph 51)
11. The Government should seek agreement with other European Union Member States to ban on demand programme services that make pornography readily available to children. We further urge the Government to engage with other international partners, particularly the USA, with the aim of securing a similar outcome more widely. (Paragraph 53)
12. We believe that, as part of its existing media literacy duties, Ofcom has an important role in monitoring internet content and advising the public on online safety. However, we are anxious to avoid suggesting a significant extension of formal content regulation of the internet. Among the unintended consequences this could have would be a stifling of the free flow of ideas that lies at the heart of internet communication. (Paragraph 55)
13. Providers of adult content on the internet should take all reasonable steps to prevent children under 18 from accessing inappropriate and harmful content. Such systems may include, but will not necessarily be restricted to, processes to verify the age of users. (Paragraph 62)
14. We have no reason to suppose that Nominet has either the resources or inclination to police the internet. Age verification, while ideal, is not the only way of preventing children from accessing unsuitable content. However, we believe that no .uk site should offer unimpeded access to adult pornography to children. This should be made a condition of registration. (Paragraph 63)
15. Site blocking is highly unlikely to be a suitable approach for adult pornography or violent material much of which is legal (at least if it is unavailable to minors) and which is prevalent on the internet. However, blocking should be considered as a last resort for particularly harmful adult websites that make no serious attempt to hinder access by children. (Paragraph 66)
16. We welcome the introduction of whole home filtering solutions that prompt account holders with a choice to apply them. We encourage all internet service providers to offer their customers this valuable service. Ofcom should monitor the implementation of this filtering and report back on its level of success and adoption. (Paragraph 74)

17. We value the UK games industry and the many educational and recreational benefits it provides to children. As filtering technologies continue to develop, as they should, we trust parents will be empowered to provide the supervision they want of what games their children play and when. (Paragraph 77)
18. We agree that the availability and performance of filtering solutions must be closely monitored, both for efficacy and the avoidance of over-blocking. It should also be easy for websites inadvertently blocked to report the fact and for corrective action to be taken. (Paragraph 79)
19. Websites that provide adult content should signal the fact clearly to enable filters better to take effect. A failure on the part of the operators of such sites to do so should be a factor in determining what measures should be taken against them. (Paragraph 80)
20. Filters are clearly a useful tool to protect children online. Ofcom should continue to monitor their effectiveness and the degree to which they can be circumvented. (Paragraph 81)
21. We welcome the introduction of ParentPort but believe Ofcom should seek to promote and improve it further. For example, more use could be made of it to collect data on complaints concerning children's access to adult material. (Paragraph 83)
22. We further recommend that Ofcom regularly reports on children's access to age-restricted material, particularly adult pornography and the effectiveness of filters and age verification measures. Ofcom is well-placed to fulfil this role given the work it does on its Children and Parents: Media Use and Attitudes Report. (Paragraph 84)
23. We note comments on the state of, and access to, sex and relationships education. We are aware this is a politically contested subject but believe the Government should take into account the views of the young people who gave evidence to us of the value and importance of good quality mandatory sex and relationship education as policy develops. In the mean time, teachers have many opportunities to use their professional judgement in advising children both on online safety and on respect for each other. We believe there is scope for providing teachers with clearer signposting of the advice and educational resources that are already available. (Paragraph 86)
24. Any changes to legislation, including consolidation of current laws, which clarify the status of bullying, whether off-line or online, would be welcome. At the same time, much could be achieved by the timely introduction of improved guidance on the interpretation of existing laws. (Paragraph 97)
25. Both Facebook and Twitter have sensible terms and conditions attaching to the use of their services. However, these should be made much clearer, explicit and visible. People who might be tempted to misuse social media need to be left in no doubt that abuses online are just as unacceptable as similar misbehaviour face-to-face. (Paragraph 100)

26. Given that Facebook and Twitter are aware of the extent to which their services are accessed by younger children, we expect them to pay greater attention to factoring this into the services provided, the content allowed and the access to both. The same applies to other social media companies in a similar position. (Paragraph 104)
27. Twitter told us that users can mark their own tweets as sensitive which by default means a warning message is posted to anyone wishing to view these. This is a good reminder that self-restraint and self-regulation are crucial aspects of any enforcement regime in the online world. (Paragraph 105)
28. In spite of reassuring words from Facebook and Twitter, it is clear that these platforms, in common with other social media providers, could do far more to signal the unacceptability of abuse and to stamp it out when it arises. (Paragraph 106)
29. Social media providers should follow the examples of Facebook and Twitter in having appropriate terms and conditions. We believe there is significant scope for such providers—including Facebook and Twitter—to enforce such conditions with greater robustness. (Paragraph 107)
30. Social media providers should offer a range of prominently displayed options for, and routes to, reporting harmful content and communications. They need to act on these reports much more quickly and effectively, keeping the complainant and—where appropriate—the subject of the complaints informed of outcomes and actions. (Paragraph 114)
31. Ofcom should monitor and report on complaints it receives, perhaps via an improved ParentPort, regarding the speed and effectiveness of response to complaints by different social media providers. (Paragraph 115)
32. We believe it is in the interests of social media platforms, if they wish to avoid a more regulatory approach, to put their money where their mouths are and provide more funding for the valuable work being done on internet safety by voluntary organisations and charities. (Paragraph 119)
33. A good deal of advice on the safe use of social media is available already. This should be signposted more clearly for teachers, who are likely to be in the front line when it comes to dealing with bullying both in the playground and in the online world. (Paragraph 120)

Formal Minutes

Thursday 13 March 2014

Members present:

Mr John Whittingdale, in the Chair

Ben Bradshaw
Tracey Crouch

Paul Farrelly
Steve Rotheram

* * *

Draft Report (*Online Safety*), proposed by the Chair, brought up and read.

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

Paragraphs 1 to 125 read and agreed to.

Summary read and agreed to.

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

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

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

* * *

[Adjourned till Tuesday 18 March at 10.00 am]

Witnesses

Tuesday 15 October 2013

Page

John Carr, Secretary, Children's Charities' Coalition on Internet Safety, **Claire Lilley**, Senior Analyst, NSPCC, **Anthony Smythe**, Managing Director, BeatBullying

Ev 1

Susie Hargreaves, Chief Executive, Internet Watch Foundation, and **Peter Davies**, Child Exploitation and Online Protection (CEOP) Centre

Ev 11

Tuesday 29 October 2013

Stella Creasy MP

Ev 20

Nicholas Lansman, Secretary General, Internet Services Providers' Association, **Dido Harding**, Chief Executive Officer, TalkTalk Group, **Hamish Macleod**, Chair, Mobile Broadband Group

Ev 28

Mr Jim Gamble, Independent Chair, City and Hackney Safeguarding Children Board

Ev 36

Tuesday 19 November 2013

Simon Milner, Policy Director, UK and Ireland, Facebook and **Sinéad McSweeney**, Director, Public Policy, EMEA, Twitter International Company

Ev 44

Tony Close, Director of Content Standards, Licencing and Enforcement, Ofcom and **Claudio Pollack**, Group Director, Content Consumer and External Affairs Group, Ofcom

Ev 52

Rt Hon Damian Green MP, Minister of State for Policing, Criminal Justice and Victims, **Mr Edward Vaizey MP**, Parliamentary Under-Secretary of State for Culture, Communications and Creative Industries and **Claire Perry MP**, Special Advisor to the Prime Minister on Preventing the Commercialisation and Sexualisation of Childhood

Ev 57

List of printed written evidence

1	Children's Charities' Coalition on Internet Safety	Ev 65
2	NSPCC	Ev 68; Ev 111
3	BeatBullying	Ev 73
4	Internet Watch Foundation	Ev 76
5	Internet Service Providers' Association	Ev 79
6	TalkTalk	Ev 82
7	Mobile Broadband Group	Ev 86
8	Facebook	Ev 89
9	Twitter	Ev 92
10	Ofcom	Ev 94
11	Home Office	Ev 103
12	Department for Culture, Media and Sport	Ev 107

List of additional written evidence

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

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

List of Reports from the Committee during the current Parliament

The reference number of the Government's response to each Report is printed in brackets after the HC printing number.

Session 2012-2013

First Report	The Gambling Act 2005: A bet worth taking?	HC 421
Second Report	Racism in football	HC 89
Third Report	Library Closures	HC 587
Fourth Report	Football Governance Follow-Up	HC 509
Fifth Report	Scrutiny of the Draft Public Bodies (Merger of the Gambling Commission and the National Lottery Commission) Order 2013	HC 1104
Sixth Report	Pre-legislative scrutiny of the draft Gambling (Licensing and Advertising) Bill	HC 905

Session 2013-2014

First Special Report	Football Governance Follow-Up: Government Response to the Committee's Fourth Report of Session 2012-13	HC 156
First Report	Scrutiny of the draft Public Bodies (Abolition of the Registrar of Public Lending Right) Order 2013	HC 506
Second Report	Scrutiny of the draft Public Bodies (Merger of the Gambling Commission and National Lottery Commission) Order 2013	HC 256
Second Special Report	Scrutiny of the draft Public Bodies (Merger of the Gambling Commission and National Lottery Commission) Order 2013: Government Response to the Committee's Second Report of Session 2013-14	HC 646
Third Report	Supporting the creative economy	HC 674
Fourth Report	Nuisance Calls	HC 636
Third Special Report	Supporting the Creative Economy: Government Response to the Committee's Third Report of Session 2013-14	HC 945
Fifth Report	Pre-appointment hearing with the Government's preferred candidate for the Chairman of Ofcom	HC 933

Oral evidence

Taken before the Culture, Media and Sport Committee on Tuesday 15 October 2013

Members present:

Mr John Whittingdale (Chair)

Mr Ben Bradshaw
Angie Bray
Tracey Crouch
Philip Davies

Paul Farrelly
Mr John Leech
Steve Rotheram
Mr Gerry Sutcliffe

Examination of Witnesses

Witnesses: **John Carr**, Secretary, Children's Charities' Coalition on Internet Safety, **Claire Lilley**, Senior Analyst, NSPCC, and **Anthony Smythe**, Managing Director, BeatBullying, gave evidence

Q1 Chair: Good morning. This is the Committee's first session examining issues around online safety and I would like to welcome John Carr of the Children's Charities' Coalition on Internet Safety, Claire Lilley of the NSPCC and Anthony Smythe of BeatBullying. Perhaps you could begin by just giving us your view of the scale of the problem now, because obviously this has been an issue that has been of concern for some time. There are measures that have been taken and there are more measures that are potentially in prospect, but it would be helpful for you to tell us first of all what the volume is, how many people are involved and how easy it is to access images of child abuse or inappropriate material. Who would like to start?

John Carr: I will go first. The question of volume is absolutely central to this whole debate. Like with all areas of crime, it is impossible to get any precision as to the real volumes. There are various straws in the wind that give us reliable indicators. The NSPCC, for example, did a series of FOI requests to all the police forces in England and Wales asking them to report back to them how many child abuse images they had seized in arrests that they had carried out in the two-year period ending April 2012. In the time frame that the NSPCC was working to, only five forces replied, but those five forces reported that they had seized 26 million images in that two-year period. I spoke to a professional statistician and he looked at them—sorry, go ahead.

Q2 Chair: On the 26 million, just to clarify in my own mind, is that 26 individuals with 1 million images each, or is it a million individuals with 26? How does it work?

John Carr: That is an extremely good point—I was going to get to it later. The numbers themselves can sometimes conceal more than they reveal. There was one man, for example, in Cambridgeshire who was arrested with 5 million images on his machine. It is not uncommon to find individuals now with a million or more images. You are absolutely right; it is possible that those 26 million images represented the activity of no more than half a dozen highly obsessive individuals who were downloading large quantities. It is very unlikely. Just to finish on the point about

numbers, because I do think they tell a story—albeit not the whole story, definitely—if you gross that up to assume broadly similar levels of activity by all of the police forces in England and Wales, that would have led you to a number in the region of 300 million that would have been seized by all police forces in England and Wales in that period.

Now, putting that on one side for the moment, we then have the revelations by Peter Davies, who I know you are going to see later today, on ITN at the end of May this year when he acknowledged that between 50,000 and 60,000 individuals had been identified by CEOP as being involved in downloading child abuse images. The period was not very clear, but none the less the key point that Davies made in that TV interview—I think it was very courageous of him to do it—was that that is simply beyond the capacity of the police to deal with this in any reasonable way. At no point since records began—for these purposes, by the way, that was around the mid-1980s—have British police ever arrested more than about 2,500 individuals for child abuse image-related offences. If you do the maths and assume that there are no new offences committed relating to images, the last individual on that list of 50,000 to 60,000 individuals who are known about now would not be arrested until 2032.

The answer is not that we simply throw our hands up in despair and say, "Nothing can be done." Something can be done, but it must involve industry in deploying ever-smarter, better technical tools to deal with it, because even if we were living in times of superabundance as opposed to times of austerity, with those kinds of volumes and those kinds of numbers of offenders, it is impossible to imagine how we would ever be able to, or want to, employ the right number of police officers, and to have the right number of prisons, courtrooms, judges and all those things to deal with the volumes that we now know exist. We have to find better technical solutions for addressing some of this.

Chair: Thank you. Just before I bring in the other two witnesses, we have two quick questions on what you said.

Q3 Mr Leech: Mr Carr, in relation to the scale of the problem, I think people would be amazed by the sheer

15 October 2013 John Carr, Claire Lilley and Anthony Smythe

numbers that you are talking about. Do you get a sense that the problem is massively on the increase, or is it simply that the detection of the problem is now far more straightforward and we are becoming more aware of what has always been a problem of this scale?

John Carr: It could be a bit of both. Certainly, obviously, we are lot better now at detecting it; we have better tools for spotting it. If we can't arrest them, at least we know they are doing it, so that definitely accounts for part of it. Internet penetration is not going to go much further, or it does not have much further to go in this country, so I doubt that mere growth will lead to increase, but we are getting better at detecting it. Around the world, that is a different picture. There are lots of countries that are coming online only now for the first time, where we can expect to see similar patterns developing. That, of course, does in a way pose a threat here, because if the volumes are increasing elsewhere on the internet, they could in the end none the less find their way to the UK.

Q4 Tracey Crouch: Mine is a very quick one. With reference to the 26 million images, what percentage were of the level 5, I think it is, which is serious, and how many were level 1? Can you give some sort of breakdown of the kind of levels?

John Carr: I do not know exactly. The data was not broken down in that way, but I would guess, particularly with volumes of that kind, that they would probably correspond roughly with the kinds of images that the IWF is seeing in general, so a very substantial proportion. I think 70% of the images that IWF deals with depict children under the age of 10 being sexually abused so, almost by definition, a very high proportion of those will be level 5 or level 4—the worst kind.

Q5 Chair: Sorry to have cut you off, but let me come back now to Claire and Anthony.

Claire Lilley: Thank you. I just want to add to what John said about the freedom of information requests that the NSPCC did, and just to emphasise that that was five forces, none of which had a large metropolitan base, so that is not including London, Manchester or Birmingham, where the figures are likely to be even higher. I just add that caveat as well. John has talked a lot about child abuse images. What I would like to touch on is the other issues and bringing the children's voice into the session in terms of what the NSPCC hears via ChildLine from children. In 2012–13, we had almost 11,000 counselling sessions from children where the main thing that they wanted to talk to us about was a problem that they had had in relation to the internet. That was a 65% increase on the previous year. In terms of what children are telling us that they are experiencing, much greater volumes of children are so distressed that they are phoning ChildLine to talk about a problem on the internet. That can be anything from online bullying, so-called sexting or online grooming—all those sorts of issues covered within that.

Specifically in relation to online bullying, for example, that saw an 87% increase in contacts from children over the last year. That corresponds with a 4% decrease of wanting to talk about face-to-face bullying. We are seeing that children contacting ChildLine about bullying is massively increasing, and obviously it is an issue about the conduct of children, but the internet and access to smart phones, tablets and all these things are facilitating and exacerbating the problem.

Chair: That probably brings us neatly on to Mr Smythe.

Anthony Smythe: Yes. I represent an anti-bullying charity and my main interest is peer-on-peer abuse, cyber-bullying and trolling. Our research would suggest that one in three children have experienced cyber-bullying. More worrying is that you will find that one in 13 are subject to persistent cyber-bullying and that is what leads to the cases of suicide and self-harm that we have seen over the recent summer months. What is the greatest concern for children and young people—and now for adults—is the feeling that they are helpless and are hopeless in terms of getting advice and support. They do not know where to go to. Our work with practitioners would suggest that a lot more needs to be done in strengthening roles and responsibilities and clarifying that so that we have an approach to tackle cyber-bullying and bullying, and realise that cyber-bullying does not always happen online. It sometimes can reflect what is happening in communities, schools and vice versa now. Children experience cyber-bullying online, and it is reflected in the playground, so you have to see those as overlapping circles with a great deal of movement between the two.

Claire Lilley: May I come back? Sorry, I meant to mention as well that I know the Committee is also looking at the impact of online adult content on children's behaviour, and I wanted to mention that ChildLine has seen a 70% increase in the number of boys contacting the service because they have been upset by online pornography specifically, so seeing pornography and being distressed or feeling guilty because they have watched it, or feeling somehow dirty or ashamed because they have seen it, whether accidentally or deliberately. Also there is an increase in children being referred to our services that we run around the country that are for children with harmful sexual behaviour and watching pornography, with easy access to online pornography, is playing a part in their sexualised behaviour.

Q6 Chair: Can you just say a little more about what evidence you have of the sort of harm that is done by children either accidentally coming across, or deliberately coming across, material that is clearly adult and should not be seen by them?

Claire Lilley: The evidence base, it is fair to say, is growing. In the past 10 years, we have seen such an explosion in access to the internet and online pornography being freely available within a few clicks—it is very easy to get hold of. While the evidence base is still growing, the NSPCC would say that a precautionary approach would be the best approach, because essentially we are conducting a big

15 October 2013 John Carr, Claire Lilley and Anthony Smythe

experiment at the minute with our young people where they have access to all this online pornography very easily and we do not know what the influence will be. We have evidence from ChildLine that children are being pressurised to watch porn by their peers and they don't necessarily want to do it. Girls are telling us that they are being pressurised to act out sex scenes from porn movies that they or their boyfriends might have watched, and there is the sexualisation of women and girls that is being caused, we believe, by these large numbers of porn being easily available over the internet.

John Carr: I will just come in on that. I think the word "pornography" when we discuss it in this context is in many ways very unhelpful, because certainly for people of a certain age, the word "pornography" is mentioned and images of a *Playboy* centrefold or pictures of ladies dancing without their bras on the beach or something spring to mind. Then this whole thing starts going about, "Well, aren't you just being a bit old-fashioned or prudish?" Whatever view you take about that, the sort of material that we are in fact talking about that is available at the click of a mouse on the internet is light years away from anything of that kind. This is, in essence, violence. It is sadistic, and very often quite bizarre.

To go back to Claire's point about the biggest experiment we have ever undertaken, porn has been around since time immemorial. Anybody who has been to Pompeii and visited the House of the Vettii can see it there in stucco on the wall. But never before, ever, including in the 1960s and 1970s, when a lot of the studies on porn were initially done, has the kind of material that is there now been available 24 hours a day, seven days a week in graphic colour, with full sound and free. In our evidence, we refer to the decision in the case of the Crown v. Perrin, which was decided in the Criminal Court of Appeal in 2002. This was a case of a man who was publishing extreme pornography on a website and had taken no steps to try to keep it away from kids. He had no age verification system—nothing in place—and he went to jail, but the judges said, "It is okay for you to publish porn. Nobody is saying you cannot or should not, but if you do, you must take steps to keep kids away from it".

That law is being honoured in the breach rather than in the observance. It is principally because most of the publishers are based overseas and the British police have not sought to extradite them or go after them, and that is a great pity. In our evidence, we have made a number of practical suggestions about how we might try to get at least companies that are based in Britain or operate from here to try to observe that particular law. That is to say, "If you are going to publish porn, okay, that is your business, but please take concrete steps to make sure kids cannot get easy access to it."

Anthony Smythe: Can I just add some statistics? In terms of bullying and cyber-bullying, the Department for Education produced some statistics a number of years ago that suggested that for those who are persistently bullied, their attainment drops by on average two GCSEs. Our research looked at persistent bullying and the link to suicides, and what we found when we looked back at the records was that 44% of

child suicides had bullying as a contributing factor. That does not mean that they committed suicide because they were bullied. It could be that they suffered a bereavement and were bullied and cyber-bullied because of the bereavement, and the totality of what they were facing led to the suicide. But it is a major contributing factor to child suicide—peer-on-peer abuse.

Chair: That neatly brings us on because Tracey Crouch wants to explore this area.

Q7 Tracey Crouch: It does. I am just going to go further into cyber-bullying, if I may, but can I just follow up on a couple of the issues that John has raised with regard to pornography? Could you just explain to me: are there already certain restrictions in place for some of the pornographic content that you were referencing, such as, for example, the more bizarre or perhaps violent images? Does that already exist, or can you just go on to any pornographic website and have easy access to the more bizarre images?

John Carr: Two clicks of a mouse. In the UK, the mobile phone networks have, since 1 January 2005, all blocked access to adult content accessible either over their own networks or the internet without you first going through age verification process. If you are accessing through a mobile phone in the UK, broadly speaking, only adults should be able to access porn in that way. But of course there are lots of other ways that you can do it. Our wi-fi providers—all the larger ones—have said that they are going to block access to porn as well. That is a great achievement, by the way. It is a world first, so we can be very pleased with that. The only people who are not yet currently taking steps to block access to those types of sites are the ISPs. But, as we know, thanks to Mr Cameron's efforts, there are currently discussions going on between all the large ISPs and the Government about introducing steps to limit access to that type of material. But right now today within the UK, there is nothing there routinely that restricts access to the most bizarre, the most violent and the most graphic types of pornography—anybody can get it.

Q8 Tracey Crouch: But is the age restriction process just a case of saying, "I am over the age of 18," and ticking the box?

John Carr: No. With the wi-fi, you will not be able to lift it—it will be fixed. By the way, that will apply only in public places where children and young people are present, so if you go to Spearmint Rhino, a casino or some place that is essentially wholly populated by adults and access the wi-fi there, you will be able to get anything that is on the internet. But ordinarily in Starbucks, at the Odeon, in a railway station and so on—places like that; public places where children and young people are going to be—you will not be able to get access to porn full stop, so you cannot prove you are over 18 and get it lifted. But with the ISPs, the process is being debated right now, and we do not quite know how that is going to pan out yet.

Q9 Tracey Crouch: But it will not impact on those accessing content at home?

15 October 2013 John Carr, Claire Lilley and Anthony Smythe

John Carr: Yes, it would. Sorry, I lost my thread slightly. The mobile phone companies have quite a robust age verification system. You have to go through the same process that the online gambling companies use, and you have either to be on the electoral roll or to have a credit card that one of the credit reference agencies can get. There are a number of bits of information they collect from you as a mobile user to determine that you are in fact an adult. What the ISPs are going to do in the end at home, we do not know. We have heard what the Government have said they want them to do. We have not yet heard from them what they are in fact going to do, and they have until 31 December to tell us. But they could introduce age verification as well, if they wanted to, because it is tried and tested technology.

Q10 Tracey Crouch: Thank you. Can I just go back to cyber-bullying, please? We heard from Anthony about the scale of the statistics and what they see as the problem of cyber-bullying. I know that both the NSPCC and yourself, Mr Carr, have referenced cyber-bullying in your written submissions as well. Could you just expand on what you are seeing from your own organisations about cyber-bullying, please?

Claire Lilley: In terms of calls to ChildLine, we have seen an 87% increase in the last year, and huge volumes of children under extreme pressure, mainly as a result of bullying from their peers. I think the characteristics of online bullying that set it apart from traditional bullying are that because children very often have phones and access to the internet at home and in their bedroom, it is not something that stops when they go home and close the door. They no longer have that sense of safety, so it is literally 24/7. Some children are telling us that if they do not respond to a message within 20 minutes at 4 am, the bullying will increase—a sort of pack mentality sometimes where it is no longer just six children involved in the bullying, but perhaps the whole year group or going out to the whole school, so the child is feeling very vulnerable in terms of their exposure, feeling a huge degree of humiliation, not knowing who knows, whatever the rumour is, and feeling it is totally beyond their control and that they are very unable to do anything to combat it. If it is happening on social networking sites, for example, it will quite often be replicated via email and instant messaging, and even if they report it to social networking sites, they often feel like nothing is being done as a result of that and that no action is being taken, so children, when it is happening to them, feeling extreme vulnerability and humiliation, and a sense of helplessness.

Q11 Mr Bradshaw: Do you take up individual cases with social networking sites at your organisation?

Claire Lilley: No, we do not, because the service that ChildLine operates is confidential, so we never disclose anything, except in the case that a child tells us that they were about to commit suicide. Only then would we breach that confidentiality.

Q12 Tracey Crouch: Section 127 of the Communications Act describes the improper use of

the public electronic communications network. Do you think that more could be made of the Communications Act to combat bullying on social media?

Claire Lilley: I would say that what bullying on social media comes down to is about behaviour. We can wave the long arm of the law at children, but what we need to do is to educate them about the impact of the behaviour in which they are engaging on people who are at the receiving end of it. We need to do much more to educate them to build their resilience, both when they are on the receiving end, but also to build their empathy and their sense of respect for other children. There may be things that we could do in terms of the law, but what we need to do is to build in much more education of children about the impact of their behaviour on others and get parents involved in talking to their children about how they behave online, how they conduct themselves and how they treat other people online.

Q13 Tracey Crouch: Anthony, do you think there should be further legislative change to combat bullying?

Anthony Smythe: I completely agree. The first priority is about prevention and education. Sometimes that does not work, though, so the question is what do you do next? What you want is a well-trained workforce around the child—a workforce that understands their roles and responsibilities and that can provide that support. As Claire says, bullying is 24/7, so we need infrastructure around the child that sees bullying from a child's point of view. For too long, we have seen bullying as a school issue or a cyber-bullying issue. Children don't see it like that. They do not have an online and offline world; it is just their world.

I would like the Government to reform their approach to bullying in the same way as they have reformed their approach to child protection, where they have seen child protection from the child's point of view and had services rallying around that child. If you do that, you will get good early intervention, and that brings in the third sector, teachers and the police. If we share the responsibility, we will reduce the workload on one another because capacity is an issue. In terms of the law, it is not fit for purpose. It does not protect children from cyber-bullying; it does not protect adults from cyber-bullying. The Children's Commissioner for Wales this morning, I believe, made a recommendation to make cyber-bullying a criminal offence. I would endorse that because I think we need to give out a message that bullying is unacceptable in our society, whether it be cyber-bullying or bullying. Under the current legislation, the Communications Act and what have you, the thresholds have been set really high. I have not seen many cases in my time where it has been used to address bullying, so I think we need updated legislation that is fit for purpose. Most of the legislation that deals with cyber-bullying was drafted many years before the likes of Twitter and Facebook. There needs to be a fresh look at this. There needs to be a legal definition of bullying, cyber-bullying and trolling because we all talk about these

15 October 2013 John Carr, Claire Lilley and Anthony Smythe

things, yet we are often working off a different definition. That needs to be embedded into legislation. In answer to your question, yes, there need to be stronger safeguards in place. There needs to be an anti-bullying strategy and an anti-cyber-bullying strategy for this country, which would set out the measures for education, prevention, intervention and support, and how we can strengthen the current criminal justice system.

Q14 Tracey Crouch: Thank you. A final question: do you think that social media providers could do a little bit more to stamp out bullying? You saw the recent very sad and tragic situation of the Ask.fm suicide and I just wondered whether you think that they should be doing more to try to prevent cyber-bullying.

Anthony Smythe: A lot of the big ones have done a great deal of work over recent years and that should be recognised.

Each time my teams that go into schools do a straw poll and ask, "What websites are you using?"—my teams are quite young people, so they are relatively up to speed with what is going on out there—they find that children and young people are using new websites and each time the dynamic of the website changes. There is a new one now where a bit of chat is posted straight away and deleted within a short period of time. The new websites are playing catch-up a great deal, and we heard a lot over the summer about Ask.fm.

Ultimately what I would want from websites is for them to know their customers. Why do people cyber-bully? First, because they can; secondly, because they haven't had the education to understand the impact it has on other people. How do we deal with the first point, which is going back to John's point about having verification about the user's identity? You can go on to Twitter and set up any account, and you can go on to all the other websites and by and large set up an account that allows you to go in and say things without fear of being suspended or caught. There needs to be a lot more done at the point of registration and a lot more investment into moderation of their websites.

I would like more transparency of the websites to hear from the big websites about how many cases of cyber-bullying are reported to them each year. What did they do about them? How quickly did they respond to those cases? What support and help did they offer? It is about having a bit more accountability. They will say that they probably do that, and if you spend five hours on the internet, you might find that information annexed somewhere. I would like that information signposted on their main websites so that parents and young people can have access and understand the website that they are using.

John Carr: Just to make a quick point, I hope. Education and awareness—what goes on between a child's left ear and their right ear—are always going to be the best defence for them in life in general, including on the internet, no question. However, let me just point you to the results of research published by Ofcom in August or September, I think: 37% of three and four-year-olds are now regularly going

online in the UK, with 9% of three and four-year-olds seemingly having their own tablets. Both those numbers are going to go up, not down. There is a limit to how much education and awareness can do in the context of three and four-year-olds.

We have a choice. We can either wag our fingers and say, "Parents, don't be so irresponsible. Don't let your kids go online at that age," or whatever, or we can accept that that is the reality of modern parenting, which therefore pushes us to looking towards the industry again for more and better technical support. Education and awareness are always the best possible option, no question, but that will not work for very young children and for vulnerable children. In that context, I think we do need to see more and better technical solutions coming into play to help.

Q15 Mr Bradshaw: Mr Smythe, you called for cyber-bullying to be made a criminal offence. Forgive my ignorance, but are there any other jurisdictions where it is already a criminal offence, or where non-cyber-bullying is a criminal offence?

Anthony Smythe: Yes. A number of countries around the world are having this very same debate. Australia and New Zealand are bringing in new legislation; Canada is about to bring in new legislation; Ireland is currently looking at it. There is an element of everyone is playing catch-up. What I would like to see is not just legislation around cyber-bullying, but a criminal offence on bullying and cyber-bullying. As I mentioned earlier, a child will be bullied in the playground and that continues online. We need to make that link because a child will not just see it as cyber-bullying; they will see it as consistent, persistent bullying. A number of countries are looking at this. Every time I have looked at a review, the recommendation always comes out to make cyber-bullying a criminal offence. I think they are just going through those procedures, so that is happening right now.

Q16 Mr Sutcliffe: It was interesting to me that the first mention of parents came in 34 minutes since you started—that was the first mention of parents. A bit of context to my contribution: I am 60 years old, and I have children and grandchildren. My oldest grandchild is 13. I am trying to come to grips, John Carr, with the size and scale of this issue. I think that Anthony's survey was in terms of one in five 12 to 16-year-olds having interacted with strangers online, and 33% of 12 to 16-year-olds going online in their own bedrooms. The size and scale of the problem is something that we need to get out into the open in terms of where we are. I do believe that there is something for the law to do, but I do think there is an issue around parenting and also content.

Again, as a 60-year-old fuddy-duddy, with the sexualisation and violence on TV now, I think the watershed has gone by the bye. If you look at some of the soaps—look at some of the storylines on *Coronation Street*, *Emmerdale* and things like that—and the violence and sexual innuendo, is there an issue for society here around how we deal with these things in terms of context and content? There are two

15 October 2013 John Carr, Claire Lilley and Anthony Smythe

questions: size and scale; and the inevitability of what is going on in terms of the availability.

John Carr: On the wider point you make about the sexualisation of society, I think with how what used to be considered unusual is now considered normal or typical, there has definitely been a shift, but however far you look across that spectrum, we are a very long way away off accepting some of the stuff that is on Pornhub or YouPorn, for example, or some of the more gross sites that are out there. They are a very, very long way from anything that you might see on a music video or at 10 am on Channel 4—or even at 1 in the morning on Channel 4. Of course the context has shifted, and things are not considered to be quite so outrageous today as they were so long ago, but the kind of things that we have been concentrating on are still way outside any spectrum of what would be considered to be generally normal.

The size and scale is part of the problem. I have been speaking to legislators and investigators as well, which is what you are now. In the past, a lot of people, when they have thought about what to do about the internet, have said, “It is too difficult. It is global. Nothing can be done”. A lot of people have a vested interest in getting everybody to believe that is true. They want people to believe that nothing can be done, that Governments are impotent and that all we can do in the end is to trust big business or all these internet companies to do the right thing. But time and time again, we see signs that they do not, and it is only when they are pressed by legislative measures or Governments very often, sadly, that they will act.

There are things that can be done. Even if every country in the world does not do them at the same time as we do, that is not a reason for us not doing them. Leadership and showing an example is also an important part of this whole equation. There are lots of things that we did first in Britain. Look at what I was mentioning earlier on wi-fi and mobile phones. We were the first in the world to do that. Does that make us mad? No. Other people will catch up; other people will copy us. There is a normative aspect of this, isn't there? There is a question about what are the right things or what we ought to expect companies to do? We ought to articulate them and our Government should press for those things to happen, however difficult they might appear on the surface.

Claire Lilley: Just on the question of parents, there is a very good tracker that Ofcom does of parents' and children's attitudes to media. Of the parents of 12 to 15-year-olds, 63% said that they felt that their child knew more about the internet than they did. I think, particularly with older children, that that is a problem, but it is a problem that we can address by encouraging parents to think of the internet as an extension of their parenting and that what they have to do is use their common sense and the same principles and guidelines that they would use in the so-called offline world and just apply those from a very early age, as the child grows, to the online world. We need to give parents confidence and empower them to think that they can deal with these issues, because the evidence does show—work by Sonia Livingstone at the LSE—that when parents lay down boundaries and guidelines for their children, children will adhere to those. That is

where the point comes in again about educating children about how to behave.

Anthony Smythe: Can I just add to that? In my paper, I said that the most useful parental control is parental responsibility. There is a need to get more information and advice out to parents so that they can have those discussions. They often feel intimidated when it comes to tech and children. They need not, because ultimately it is about, as Claire says, having those discussions about empathy for other users online and being responsible online. Often you find with cyber-bullying that they don't often realise the damage on the victim—the person on the other end of the bullying. When you address that, they start to change their behaviours.

Q17 Mr Sutcliffe: On that, Anthony, in your survey, 22% of 12 to 16-year-olds thought that being bullied online was part of life. It has become the norm, hasn't it, in terms of there being an acceptance of bullying by that 20%?

Anthony Smythe: I found that statistic to be quite sad because they have just given up and we need to make bullying and cyber-bullying unacceptable. The reason why people tend to troll and join in with the cyber-bullying is because they feel it is okay to do it. Again, it goes back to that programme about education, about empathy for other people online and about the fact that it will have an impact on that person. You may not be the only person saying it; you may be person No. 1,000 and they have probably been hearing that abuse for six months or a year. That is why we see the self-harm. That is why we see, unfortunately, in recent months, the suicides. We do need to educate people online. The internet providers have a role in there in the social networking sites. They also have a role pointing users to help and support that they can get as soon as they make a referral to them. My charity has counselled over 3,000 children over the last year on bullying and cyber-bullying, but I have not received many referrals from the big internet or social networking sites—they come to us direct. That is something we need to improve on.

Claire Lilley: I would just like to build on that by saying that in terms of educating children about these issues, it is definitely parents, but also the industry. There is a lot more they could do in terms of the number of human moderators they have enforcing their terms of service, being very clear about what their terms of service are, having terms of service written in very basic language that is child-friendly—all these things—and being much more transparent. At the minute, we have no idea of how many reports they are getting of online bullying or online grooming per year. They could be much more transparent about what they are seeing and what they are doing to deal with it, and about what the rest of us could do in partnership with them to help deal with it as well.

Q18 Angie Bray: If I could just continue a little bit along the lines of my colleague, Gerry Sutcliffe, about the role of parents in this, because what I see at the moment is an army of people marching into family life, in a sense, whether it is the Government or organisations like your own. It is changing laws and

15 October 2013 John Carr, Claire Lilley and Anthony Smythe

having to put filters on this, that and the other—which is information to other people—all because effectively, it would seem to me, you are saying that there is a shift in the relationship between parents and their children. Call me old-fashioned, but there was a debate many years ago about whether children should have televisions in their rooms precisely because of what they might be watching that was not being monitored. Fundamentally, isn't the point that parents should have the confidence—I understand what you are saying about online and internet and all that—as they have done in the past and make the time to take an interest in what their children are doing in the privacy of their own rooms, however intrusive they might be worried that might seem to be?

Claire Lilley: I think that is the ideal scenario: parents who are engaged, who are confident, who understand their children and who make time for their children. Unfortunately, that is not always the reality. Some parents are not confident and don't feel equipped, and there are some children who, as a result, are particularly vulnerable. There are also children who do not have an active adult in their life, or perhaps their parents might be substance misusers, for example. There are quite a lot of children in that bracket. I think we have a duty to spread the load. Parents definitely have a big role, but there is a lot that the rest of us can do. We have mentioned the sexualisation of society. It is a broader problem than just within families and the family unit; it is a problem for the whole of society, so we all need to play a role in that.

Q19 Angie Bray: I take that point, but fundamentally the family unit is there. It is, most people would argue, the most successful start for a child's life. I just feel that the stress is now all on what the state can do to deal with this problem, but there is much less about what can be asked of parents to take responsibility for their own children. I wonder whether your messaging should not start by talking about parents, rather than talking about changing laws and applying more regulation. Shouldn't it start, where it possibly can—I accept that it cannot always—in the home with a proper relationship, where the parents expect to be able to go in, knock on the door and say, "Hi. What are you up to this evening?"

Claire Lilley: Yes, absolutely.

John Carr: First of all, a lot of this activity is not taking place in the child's room. Bear in mind that internet access is now essentially ubiquitous. You can walk out of your house with a tablet, a mobile phone or a games console and connect to the internet essentially anywhere. The things I was referring to earlier about the wi-fi providers are an example of them doing the right thing and essentially helping parents to create an environment that they would want their children to be in. What parent would be happy with the thought that their child can go into a restaurant or Starbucks and sit next to a dirty old man looking at porn on his laptop? Nobody would, because there is a reasonable expectation that that type of material ought not to be in public view in places where children and young people are going to be.

It is why we have had rules and laws about this type of thing in relation to cinema, for example, and there was for a very long time. In a way, some of the things that we are describing are us as a society catching up with the consequences and impact of the new technology, and trying to recreate in the virtual space rules and laws that we have had—not quite since time immemorial, but certainly for a very long time. I do not hear anybody arguing, for example, that we should get rid of the rules about 18-rated movies and make them open to everybody and anybody. In essence, all we are doing—certainly when you talk about porn—is trying to recreate in the reality for children's lives, which is a virtual one, the same rules that we have applied for a long time in cinemas.

Another aspect of this as well, by the way, is the knowledge gap. There was a debate many years ago about whether it should be legal for parents to buy their children a computer or a mobile phone until they had passed a test like for a driving licence or something to show that they had at least a rudimentary understanding of the types of things they were handing over to their kids. That never got anywhere. Certainly the industry did not like the idea that this could act as a brake on the sales of these brand-new shiny devices. We absolutely put parents front and centre, but what we also acknowledge is that, particularly because of the speed at which these things have changed, a lot of parents—even very dedicated, loving, nurturing and supportive parents who would fit any ideal paradigm that you could construct—feel they need that little bit of extra help, and that is where I think the state can play a role.

Q20 Angie Bray: What you are saying fundamentally is that this new technology has fundamentally altered the relationship between parents and their children because it is—

John Carr: The same potential for control and intervention simply does not exist. Some parents think, "Oh, little Johnny is up in his room. He is safe. He is upstairs. He is not out on the street playing with the bad boys and the bad girls. He is not behind the bicycle shed smoking. He is up in his room online." In other words, there is a fundamental gap in the knowledge that we need, and a lot of this you can see as a way of trying to help bridge that gap.

Anthony Smythe: I can only repeat what John just said. Even the best parents need help and advice in terms of addressing this issue and having those conversations. Ultimately, I do not think it is for parents alone to do this. Peer-to-peer support is sometimes the best way to tackle online abuse. The approach cannot be top-down, because top-down approaches from Government probably will not work, but we do need better leadership so that we can help to clarify roles and responsibilities so that when a child is cyber-bullied in the middle of their summer holidays, either the child or the parents know where to go to get support, to feel safe and for that cyber-bullying to stop. I do not think that scenario is an easy one for people to answer yet. The Department for Education did a lot of good work in terms of clarifying roles, responsibilities and powers for head teachers to deal with bullying in schools. We have not

15 October 2013 John Carr, Claire Lilley and Anthony Smythe

seen the same in terms of cyber-bullying, and while it would be good to get that leadership, it needs to involve everyone—it cannot be top-down. It needs to be a conversation; a joint plan, if you like.

John Carr: Sadly, many of the big internet companies that are not British—they are not based here; their jurisdiction is elsewhere—do need to be encouraged, let us put it that way, to act. No business that I have ever heard of willingly steps up and says, “Please regulate me. I do not know what to do, so please would you, Government or politicians, tell me what to do?” They do not do that. Businesses will go on ploughing their own furrow unless and until something cuts across their pathway. That is what we do, in essence. We try to raise these issues and that is what Governments do as well.

Q21 Steve Rotheram: Just following on from Angie Bray’s questions, it would be fantastic to believe that all parents are responsible and do have that relationship with their children. While I genuinely believe that education and awareness are primarily the ways to tackle the issue, that is not always the case. There are parents who are absolutely fearful of IT and do not understand it, and therefore do not understand the content that can be accessed via it. But you also mentioned that there are potential technical solutions to it. There are flash screens that can come up that say you are about to access a site of adult content or whatever. There are restrictions that can be put on to these, such as for anything that is over 18, you have to opt in rather than out of it. There are blockages, I believe, that you can do to adult content coming into the home. I do not think this is all an either/or solution.

John Carr: Correct.

Steve Rotheram: I think with the education, fantastic, but there may well be other things that can be done. What are the most effective ways and what more could be done to curtail children’s access to adult content or age-restricted material, including pornography and graphic depictions of violence?

John Carr: We have never said that porn should not exist or should not be on the internet. If it is legal, there is no reason why it should not be published, but companies that make pornography available should take steps to make sure that kids cannot access it. They should employ age verification. The British gambling industry has done it with tremendous success. We never hear of cases of kids getting online and gambling. Why? Because Parliament, through the Gambling Act 2005, introduced a law making it obligatory. The Gambling Commission can give you a licence to operate as an online gambling company only if you prove to the commission that you have an age verification system in place that works and that is robust. That could be done in any other area, including this one.

There are technical tools available, but they are not being used—they should be. I do not want to argue against myself because I am a great believer in technical tools helping parents to put in place stuff that they would want, even if they do not know that it is what they would want, if you see what I mean. Technical tools can do a great deal to supplement

good parental support and guidance. They will never be 100% perfect. Nothing in life is 100% perfect. No self-respecting parent would delegate their parental responsibilities to a piece of software, but they definitely can help, and in some situations that software might be the only help that exists to keep that child safer than it would otherwise be. There are tools available. They can be done. They will not solve everything, but they could do a lot to help.

Claire Lilley: Just to add to that, one of the arguments we hear against the use of these parental controls and against the active choice or the opt-in is that it will lull parents into a false sense of security. If that is the case, as John has said before, there has been an awful lot of non-lulling going on for a long time. The parents who are already using these parental controls are the parents who are already engaged and therefore are not complacent and probably already doing a range of other things to support the use of those tools, like having conversations with their children and looking at their children’s browsing history and so on. But for the parents who are not already having those conversations and not already using the tools, the opt-in system will provide a nudge to make them think about it and engage with this subject, so we think that is valuable.

Anthony Smythe: My main concern with filtering is that there is a danger it may filter out useful information for children and young people, so it could be information on sex advice or health conditions and so on, such as anorexia.

John Carr: But that is bad filtering.

Anthony Smythe: That is bad filtering, but there is a risk that it will happen. The most important thing we can do regarding technology in terms of social networking sites is for social networking sites to know who is on their site at any one time and to have that verification in place so that people cannot set up fake websites, because it is those fake websites that allow you go on and abuse others without fear of being caught. If people knew that there were stronger laws in place and that they could be traced online, they would behave differently. The filtering is fine to a certain degree, as long as it doesn’t block useful information. What filtering will not do is prevent peer-on-peer abuse.

Q22 Chair: How exactly do you envisage that happening? Anybody can set up a Facebook account with an alias just by creating an email address. What more do you expect them to do?

Anthony Smythe: That is my concern—that it is too easy at the moment. John has mentioned how it has been done in other parts of the online world. We need to look at that age verification. I know DFE was doing a lot of work in looking at ways to take that forward. Ultimately, I think that is a job for industry to take forward. They are earning billions and billions of pounds. They can find a way, I am sure, if they were told to and this is where pressure from Government would be useful. But as a starter for 10, it may be the use of credit cards—that type of thing—so that you know who that user is and that they are at a certain age. At this moment in time, for example, in my charity, we have a Twitter account for our resident dog

15 October 2013 John Carr, Claire Lilley and Anthony Smythe

and that is how easy it is to set up these accounts. There is no point threatening somebody that you will suspend their account because they know they can set up a new one straightaway. We just need to review the whole situation.

Claire Lilley: Some of these sites need more human moderators to look for the fake accounts. That is one part of it, but they also have very sophisticated algorithms where they look at what language people are using, what sites they are visiting and what they are talking about online. They can tell with quite a degree of sophistication a lot about the individuals. Twitter, for example, has a minimum age of 13, but when you sign up to Twitter, you do not have to put in your date of birth. There is nothing to stop you. Twitter would say that what it does is to look at its algorithms to spot the children who are under 13 and therefore potentially on a site that is aimed at an older audience and containing information, posts and so on that are not suitable for their age. Its argument is that it uses very sophisticated algorithms, so I think there is a lot more that the sites could do.

John Carr: I will just make a fairly obvious point. The abuse of anonymity lies behind most of the enduring problems on the internet that we are concerned about. I do not care if people sign in as Donald Duck or Ronaldo or whatever. What matters is not how you sign on, and not necessarily how you present yourself in a public space on the internet, but that you are traceable. If people were traceable and knew that, should they cross a certain line, the cops, the courts or whatever could fairly rapidly ascertain who they were and reach out to them, I think that would have a tremendously beneficial effect across the internet in all sorts of different ways.

Of course immediately you then get thrown back at you, "What about political dissidents in North Korea? What about whistle-blowers? What about people dealing with sensitive subjects of one kind or another who need or can benefit from anonymity?" Two things to say about that: I have no desire to make it more difficult for political dissidents in North Korea to overthrow their Government, if that is what they want to do. I have no desire to make it harder for whistle-blowers to do their public service or for people who deal with sensitive information. But it cannot for ever be a question of either you make your children safer, or you make it impossible for political dissidents to log on.

Q23 Chair: So how do you do it? What is it that you would like to happen?

John Carr: One potential route would be to develop a trusted third-party institution of some kind in whose integrity one could have a very high degree of confidence that could issue IDs that would not be disclosed to anybody unless and until due process had been followed. If you were dealing with a sensitive health issue or you were a whistle-blower, or if you were a political dissident in a particular country or whatever—although God knows, after the revelations of what the NSA gets up to with Mr Snowden, whether you would ever trust the internet again anyway—you would be able to be behind a shield of

anonymity without putting yourself entirely beyond the pale.

Q24 Chair: So you have that, but what I am asking is what are you expecting Facebook, for instance, to do to satisfy themselves?

John Carr: Sorry, right. So the requirement on internet service providers would be to verify that the individual who has just signed up with them is not in fact a dog, but an actual human being with an actual and verified address where they can be reached. That alone would act as a major brake on a lot of the bad behaviour.

Q25 Chair: At the moment, I go on to Facebook and call myself Donald Duck, I have created donaldduck@hotmail.com or whatever—

Steve Rotheram: No, I did Donald Duck.

Chair: Oh, Steve has Donald Duck. But whatever it is, I have a Facebook account. What is that you want Facebook to do before signing me up?

John Carr: What the gambling companies do now is to say, "If you want to place a bet, that is fine; that is what we are here for. We just need to check that you are who you say you are". They ask you for various bits of information—four or five different pieces of personal information that they confirm—and assuming everything holds up they give you your account. You can then call yourself Donald Duck; it does not matter. That particular Donald Duck will be traceable back to John Whittingdale, SW1 and you will behave accordingly, one assumes.

Q26 Chair: Do you think there is any prospect of Facebook or Twitter agreeing to do this?

John Carr: Not voluntarily, no, but with all the revelations Mr Snowden has made and continuing escalation in criminal behaviour online, and law enforcement around the world feeling more and more beleaguered and besieged, I do not think the current situation is sustainable in the very long run. Will big companies on the west coast of America seek to resist this? Yes, they will. It will be a tussle of will between political institutions and Governments as to who wins that battle or how quickly it will be won, but I have no doubt the current situation is not tenable in the long run.

Q27 Steve Rotheram: Chair, I think there could be an evidence session just on that one aspect of what we are looking at. I have met Facebook, Twitter, the police, the Home Office and the DPP on trolling as an issue. I thought I had a simplistic solution whereby the verification could be done with somebody's national insurance number, but it costs to go through the verification process and the likes of Twitter and Facebook are not prepared voluntarily to cost themselves several billions of pounds because there are literally billions of people who are on social media platforms, so it would take something from the Government to force their hand.

There are also issues of death threats and certainly rape threats that happened to a Member of Parliament, and the algorithm did not quite pick that up because it was a little bit more subtle. There were issues about

15 October 2013 John Carr, Claire Lilley and Anthony Smythe

that, so that had to be monitored by an individual over a two-week period and somebody was arrested for that. The laws are in place. The laws around this are very complex. We have picked up on seven different pieces of legislation that can be covered for what happens online and offline, so it might be time for Parliament to look at this as an issue and to take it seriously. There is something called the Trolling Academy that promotes individuals specifically to troll MPs, for instance. After this, who knows? We might all get what I got last time I mentioned this, which was lots and lots of Twitter feeds or whatever they are called—tweets—and Facebook feeds on our statuses attacking us. But there you go, that is part and parcel.

If we could just move on to the issue about child abuse images, given that these images are illegal throughout the world, to what do you attribute the apparent prevalence of the material that was mentioned before? Was it 300 million pieces that are known to exist in the UK alone?

John Carr: I think it is a profound shock to realise that so many people are interested in that type of material. There is an appetite for it and people go and get it, and they circulate it. They are getting away with it because we do not have the capacity to stamp it out.

Q28 Steve Rotheram: We do not have the capacity.

John Carr: We do not at the moment, for sure. I do not know if Peter Davies has arrived in the room yet. Look at Peter Davies' interview on TV at the end of May. He said he would like to arrest all 50,000 to 60,000 people who CEOP had identified as being involved in exchanging or trading these images, but that is not the situation we are in, so they go after the—

Q29 Steve Rotheram: Is it lack of capacity or resource? We have the ability, because we can detect them.

John Carr: I suppose if Peter had 100,000 police officers and an unlimited budget, he could probably get them all, but we have not, and I do not see any scenario where that is going to happen.

Claire Lilley: The internet has caused a huge growth in the number of people who are looking at these images. It has removed a lot of the key inhibitors that would have once stopped men looking at it. You can now get these images completely anonymously, they are free or very affordable, and they are very easily accessible. Because of those three things, we have seen a growth in men—it is usually men—who once would not have gone down this route, but now they are looking at it. That is why the NSPCC believes there is a need for a public education campaign. From studies of offenders, their motivations and the reasons why they have done it, quite a lot of them will maintain that they have not done anything wrong, that it was just an image and that they did not touch a child, so they did not actually commit child abuse. We need to educate people that these are not just images; that by looking at these images, they are committing an offence; that a child is being re-victimised every single time an image is looked at; and that they are potentially affecting their own sensitivity around the

issue and escalating their own ability to go down that route and end up abusing in the physical sense themselves. There is quite a lot of research now about the crossover between non-contact and contact offending and CEOP would put it at about 50%. There are a couple of studies that put it at between 40% and 55%, which is a very high level of crossover. It is not just looking at an image; it is much more dangerous than that.

Q30 Steve Rotheram: You said that they are easily accessible images. Does that in some way excuse the fact that people might innocently stumble on them? My understanding is that it is not easy to click on something and then for these graphic images that we are talking about, even though there are 300 million of them, to be readily accessible—there are other things that you would have to click on to. So if you just put a name up or something and a whole list of images came up, they would not be of the graphic nature, surely, of child images.

John Carr: It depends. You can get pretty quickly to some of them. Some of the ostensibly legal adult sites will have sections with names like “jail bait” or “barely legal” and very often that is a code for saying if you keep going just a couple of clicks through there, you will find stuff that is not legal and definitely is jail bait. If you go on to peer-to-peer networks, you can type in certain words and pretty quickly get at them. You are right that you need a little bit of determination, but not a great deal.

Claire Lilley: Anyone who innocently stumbles across them accidentally should be reporting them immediately to the IWF. Lots of people do, though not everyone by any means. I am sure the IWF will talk about that in the next session.

John Carr: Just be clear, we are not blaming the internet for this. People do things, not machines. What the internet has done is open pathways that have allowed people to walk down them in a way that just was not there before. That is the shocking and surprising thing—the numbers of people who have decided to walk down that path.

Q31 Steve Rotheram: But internet providers cannot abrogate responsibility completely for those images being on their systems. Surely there must be some people who could block those images.

John Carr: Absolutely; I 100% agree. We do have a fundamental issue with the law, of course, which is that the EU-wide e-commerce directive expressly says that you have no legal liability or responsibility for anything on your network unless and until you have actual knowledge of its existence. Some companies take that as a get out of jail card. They say, correctly, “We are not accountable. We cannot be prosecuted or pursued for failing positively to go forward to try to block things.” To their credit, many choose to, certainly in the UK, but not all do. That is because our law says there is no liability for this material online unless and until you have actual knowledge.

Q32 Steve Rotheram: Even though the content itself is illegal.

15 October 2013 John Carr, Claire Lilley and Anthony Smythe

John Carr: To be honest, they must know that that illegal content is on their network, but unless they have actual knowledge of it, they cannot be held liable. I get that, up to a point—you cannot find somebody guilty of something if they do not know specifically that it is there—but I think it is a shield that scoundrels can hide behind. We ought to simply acknowledge that this stuff is out there and there should be an expectation that companies running internet access providing services or internet ISPs ought to have an obligation to try to intervene to minimise or reduce this type of material, even if you do not hold them legally liable.

Q33 Steve Rotheram: Do we know how many sites or images are taken down on a regular basis?

John Carr: You have the IWF appearing in a minute.

Chair: Absolutely; that is for our next panel.

Claire Lilley: Just one last point. There is a lot of information we do not know and one of the things that we do not have in this area is some sort of high-level strategic information-sharing forum. There is a lot of partnership working going on, but there is no one place in which it is held in the same way as I believe there is for terrorism, for example. We obviously have UKCCIS, but it does not deal with child abuse images online because it largely takes the view that those are illegal and therefore that is dealt with. I think we do need some sort of more strategic forum at which industry—CEOP, IWF, everyone—gets around the table and shares information and best practice about what can be done.

Chair: That very neatly leads us to our next panel, so may I thank the three of you very much?

Examination of Witnesses

Witnesses: **Susie Hargreaves**, Chief Executive, Internet Watch Foundation, and **Peter Davies**, Child Exploitation and Online Protection (CEOP) Centre, gave evidence

Q34 Chair: May I welcome our next two witnesses: Susie Hargreaves, Chief Executive of the Internet Watch Foundation, and Peter Davies, the Chief Executive of CEOP?

Perhaps we can continue from the point we reached with the last panel: can you first of all give us your idea of the volume, the scale of the problem and the number of people who are involved; and perhaps address Claire's point about the need for greater co-ordination in gathering information?

Peter Davies: After you.

Susie Hargreaves: Thank you very much, Mr Chairman. Would it be useful if I just gave a brief summary of how the IWF works and the key areas in which we operate?

Chair: Yes.

Susie Hargreaves: The IWF is the UK hotline for reporting criminal content, specifically child sexual abuse content hosted anywhere in the world, non-photographic images of child sexual abuse hosted in the UK and obscene adult content hosted in the UK. We are a self-regulatory body founded by the UK internet industry 17 years ago. We are an independent charity with an independent board and independent of law enforcement and Government. Our operations are covered by a memorandum of understanding with the Association of Chief Police Officers and a service level agreement with CEOP. We work very closely with CEOP on a day-to-day basis. Very quickly, we are funded by the internet industry—80% of our money comes from them and the remaining 20% comes from the EU as the Safer Internet Centre for the UK along with Childnet International and the South West Grid for Learning.

Specifically, the way we work is that we currently take reports from the public—although this is about to change—and assess those reports, and if we find that child sexual abuse content is hosted in the UK, we issue a notice and takedown. We typically have the content removed in under 60 minutes. If it is hosted outside the UK, which the majority are, we notify the

sister hotline in that country or international law enforcement, and until such time as that content is removed, we place it on a blocking list, which is used across the UK and in many other countries. It is a very dynamic list and it is updated twice a day, and the content stays on the blocking list until such time as it is removed at source. The most effective way to remove content is to remove it at source. It is our view that blocking will only stop inadvertent access and will not stop the determined. We also have a keywords list.

My final point is to say that 17 years ago, when we were founded, 18% of child sexual abuse content was hosted in the UK. It is now down to less than 1% and that is because of the tremendous relationships we have. It is about partnership working. It is about the UK and international internet industry, and our relationship with law enforcement, the Government, the public and civil society.

To answer specifically your question about the extent of the problem, the truth is that nobody knows how many images are out there. John has mentioned a number of images, but we do not know. Nobody knows how many unique images are out there. The majority of the images we see are duplicates and I imagine that the majority of the images within those numbers that John quoted were also duplicates. To give you an indication, we see about one to two new images a week. The scale of the problem to us is that last year we had about 40,000 reports of which we actioned just under 9,500 individual webpages. A webpage can contain from one image up to thousands of images or videos. Of those just under 10,000, 35 were hosted in the UK. In terms of the type of content, 81% were of children who appeared to be 10 and under; 4% were under 2; and 53% were levels 4 and 5, which are the rape and sexual torture of children.

Q35 Chair: Just before Peter Davies comes in, I have a couple of questions. You said one or two new images a week. That does not sound very many, given

15 October 2013 Susie Hargreaves and Peter Davies

that previously we have been talking about millions and millions of images. These are just the same images being circulated round and round? You are not suggesting that only one or two new images are taken every week; it is just the ones that you happen to stumble across, is it?

Susie Hargreaves: Yes. The majority of images that our analysts see are images they have seen many, many times because images are recirculated. This is one of the issues that we try to get across, particularly in terms of young people's behaviour on Sex Teen, is once an image is out there, it is out there for ever because it will just be recirculated and redistributed. What it means is that when we do see a new image, we can immediately work with the police to notify them, because if it is an unidentified child, we can say it is a new image and pass it on to the police.

Just also to clarify, our role is around the removal of content, and we pass on and share intelligence with the police, but we are very much not part of the police side of the work. We are not about the child protection side or the safeguarding of that child, or in fact the investigation of the perpetrators. But in terms of the new images, we see very few new images, but we see an awful lot of recycled images.

Q36 Chair: You said the best way of dealing with this is at source and that you talk to your sister organisations. But in the world where there is no equivalent of you, where people are likely to host this material, are the particular countries where it is hosted that you cannot get to?

Susie Hargreaves: There are 42 hotlines in 39 countries. The majority of them are in Europe and North America and Australia—those sort of countries. We are working with the Commonwealth and with ITU, the UN International Telecommunications Union, to look at ways in which we can provide a back-office solution for countries without a hotline where they are having increasing internet penetration to be able to report. We provide them with some support to do that, because what we are seeing, as John Carr talked about, is that as internet penetration grows in developing countries, people are starting to access these images.

In terms of where the content is hosted, about 50% of it is in North America—the US and Canada. We are seeing less content hosted in Russia than we saw in previous years. Patterns change slightly—we are seeing some emerging markets out in Asia, Cambodia, Vietnam—but the majority is hosted in the United States.

Q37 Chair: Yet the United States presumably has pretty tough laws about this, does it not?

Susie Hargreaves: One of the reasons we are so effective in the UK is because we self-regulate, so we do not have any mandatory powers to enforce internet companies to remove the content, but they do it on a voluntary basis, which means they can remove the content very quickly. In the States, internet companies are obliged to notify the National Centre for Missing and Exploited Children—Peter will be able to answer this much better than I can—and they then have to go through a quite lengthy judicial process to have the

content removed. That means that it takes a lot longer. Since we have been in operation, it used to take 20 days to remove the content in the US. It is now down to 10 days. We are working very closely with them. We now have permission to go directly to organisations that are members of ours and are based in the States and simultaneously to alert them to the fact that they are hosting content at the same time as we tell the police in the States. We are trying to bring that time down, but it is to do with the judicial system and how law enforcement works in the States, but I defer to Peter's expertise on this.

Q38 Mr Bradshaw: You just implied that the speed of taking content down is part of the reason why a lot of it is hosted in the US. Did you mean to suggest that connection?

Susie Hargreaves: No, I do not mean to do that. The reason why a lot of it is hosted in the US is, first of all, that a lot of companies are based there. The internet industry is very big in the States. Also, there is all sorts of legislation around freedom of information and ability to host certain sites, which is to do with their judicial systems. But, Peter, you would probably answer that better.

Peter Davies: Chairman, thank you. Should I perhaps wind back to an introduction, if that is okay?

Chair: Yes, I think that would be helpful.

Peter Davies: But I will happily address any questions raised. I am grateful to Susie for leading off.

My name is Peter Davies. I am now the Director of CEOP, which is one of the four commands within the National Crime Agency, which commenced last Monday, 7 October. The CEOP centre has existed since 2006 and was previously affiliated to the Serious Organised Crime Agency. Our mission, whether as a centre or as a command, as we are now, is to protect children from sexual exploitation and sexual abuse. When we were founded, there was heavy emphasis on online protection. Our remit does not limit us to online activity, but what we try to do is to become a national hub for intelligence, a national contact point and a source of expertise and specialist support on any aspect of child sexual exploitation that would benefit from that approach. We still have a very strong heritage and a very high level of expertise in child abuse imagery and other related forms of harm.

Our threat assessment, which is published every year, was most recently updated in June this year and in that we identified four key threats to which we address our minds, two of which are specific to online. One of those is the proliferation of indecent images of children. Images, as I am sure you will know, are a harm in themselves. They are scenes of crime. They are depictions and recordings of children being very seriously raped and sexually abused and the possession of these is a crime—and rightly so. The possession of these is also, as Claire Lilley referred to, quite a strong indicator of a sexual interest in children that also extends to physical abuse, and so anybody who possesses indecent images of children is a criminal, but is also somebody who might present an additional risk to children, as if that were not enough.

15 October 2013 Susie Hargreaves and Peter Davies

I can go back to talking about the overall level of prevalence, but I also want to highlight the other aspect of threat that we are very concerned about, which is what we call online child sexual exploitation. This is less well understood. I would not estimate the prevalence of it, but what we can say is that this appears to be an emerging trend of offending and its consequences for the victims extend to fatal consequences and are in many cases very severe. This is not so much about taking an interest in indecent images of children as about using the medium of the internet to contact, ruthlessly manipulate and exploit and sexually abuse children to the point of causing them physical and psychological harm, and in some cases pushing them towards suicide either because of the acts they have been compelled to do, or in some cases because they have carried out acts online that are then used to blackmail them for money—money they do not always have. So these are the two key areas of threat.

We have excellent relationships with a number of external bodies, including the Internet Watch Foundation, which I think is a world-leading organisation at doing what it does.

Our remit does not extend to all the issues that I know you are examining because we have to focus in. Everybody has a view about the risks associated, for example, with children accessing adult pornography online. We have to restrict our interest in that professionally to the extent to which it makes them more vulnerable as victims, or maybe increases the possibility that they will be offenders in future.

Turning to prevalence, on the second threat I referred to, online child sexual exploitation, we do not know and we would not pretend to know. We deal with a number of cases, and a growing number of cases, of increasing severity. The type of offending is hugely harmful and also complex to investigate because it necessitates no physical contact at all between the offender and the victim. It is not uncommon for us to encounter situations where offenders in one country will target and harvest victims in a completely different part of the world. The complexities that presents are obvious. But we do not know how much is going on and it is in the nature of any form of child sexual abuse or exploitation that it will be under-reported by the victims because the whole process is designed to minimise the risk that they will report and designed to induce shame and embarrassment and all the things that might stop a young or vulnerable person coming forward and saying what has happened to them.

Q39 Chair: Where is it principally happening? Is it Facebook?

Peter Davies: It is important to identify that what we are trying to tackle is appalling aspects of human behaviour, to some extent facilitated by the internet. At the moment we are seeing roughly half of this kind of activity—online child sexual exploitation—taking place through social networking sites. Of course Facebook is a major one, but not the only one. We are also seeing it taking place through chat environments and other forums. But it is important to realise, as I think John Carr said previously, that the medium is

not to blame. The medium might be managed better so that it is safer for its users, but what is to blame is human behaviour, albeit through the internet amplified, multiplied and in some cases almost industrialised to a quite remarkable degree.

In terms of the proliferation of indecent images of children, we are a little bit clearer about this. I would not estimate a total number of indecent images circulating on the internet; I would not estimate the number that are duplicates or unique. I would probably observe that regrettably there are more now than when you started sitting this morning and that is one of the major challenges that we have. You don't need me to explain what has to happen for an image to be created.

Q40 Chair: That does not quite equate with the one or two new ones a week, if you see what I mean.

Peter Davies: Our experience is different, because of course we are a different organisation and we receive reports through different routes. It is absolutely true to say that the majority of images that we encounter are repeats. I do not have a figure on the proportion that are new, but a lot of our investigations are not so much into the images themselves but into the child abuse they portray or the child abuse that they give us an opportunity to interdict, and so it is understandable that we may not come up with the same figure. As I say, I would not estimate the total number circulating. There are always more being produced and obviously that again is a harm in itself.

Where we have got somewhere as a centre over the last two years is getting a sense of how many offenders there are in the UK, and I think John Carr has already referred to this. In our thematic assessment published in June, we estimated that there may be around—I use that term carefully—50,000 people in the UK who commit offences at least to the level of possessing indecent images of children, which is quite a stark figure to contemplate. But I am firmly of the view that it is not enough to deal with a handful of cases—and deal with them well, which I believe CEOP and our colleagues in law enforcement, supported by our partners, do—but have a sense of the overall scope of the problem, because it is that sense of the overall scope that drives a lot of other people who can help to want to do something as well. I would echo roughly what Susie says about the trends in images. We check trends in images every year and our experience recently has been that the victims appear to be getting younger and younger and the level of abuse portrayed appears to be getting worse and worse. So there is no comfort in any of these aspects of our analysis.

In terms of reporting, if I may just cue in based on Susie's point, we do receive reports from the Internet Watch Foundation. We have a very clear service level agreement and we are looking to revise and update that into a collaboration agreement very shortly. We are keen to work together with the IWF every step of the way. We also have partnerships with other organisations that report incidents to us, the most high-volume one being the one that Susie referred to, which is the National Centre for Missing and Exploited Children in the United States, from whom

15 October 2013 Susie Hargreaves and Peter Davies

we receive on average maybe 800 reports per month. We also have reports from UK organisations including, very importantly, the IWF. We are also available for any member of the public who wishes to report any concerns to us online. That public reporting has probably doubled in volume over the last year or year and a half, and we generally expect 300-plus reports into CEOP online from the public every month about incidents of concern.

Susie Hargreaves: Mr Chairman, could I clarify the issue around the number of new images? When we talk about new images, it might be a series of images, but you have to remember that that means two new children who have been sexually abused. So it is not just an image, it is two new children who have been sexually abused in itself, and it will be the worst of the worst stuff.

Also, I just wanted to say there is a lot of information out there about potentially how many images there are and of course it is a changing field from day to day, but I do think there is still a need for some very robust research. I would certainly echo what Claire was saying earlier on. Although we have the UKCCIS board, of which we are both members, that is very much around the whole field of child internet safety and online protection. In the field of online child sexual abuse content, we do need a kind of high-level strategic thinking body to get together a couple of times a year to start to share that high level of intelligence. It only works in the UK because we work in partnership and all do our specific bits, but it is really important that we understand the whole and the context.

Q41 Mr Bradshaw: If most of this content is being generated in the States, who are these children? Have they been—

Susie Hargreaves: Sorry, could I clarify? It is not necessarily generated in the States; it is hosted in the States.

Peter Davies: If I can help, the process by which it is identified is a specific piece of legislation that exists in the United States called the Protect Our Children Act 2008. It places an obligation on communications and internet service providers to identify and report to NCMEC, the National Center, incidents that appear to depict child sexual exploitation. There is a piece of legislation in the States that places this obligation and it is in the discharge of that obligation that they report everything—well, the performance varies, but they report things to the National Center and the National Center identifies the location of these through internet protocol addresses and so on. What we receive in the UK is effectively, for want of a better expression, the UK slice of all that which is reported to the National Center.

Q42 Mr Bradshaw: So where is it being generated? Who are these children? Have they been kidnapped? Are they within families?

Peter Davies: It is hard to tell. There is one more thing I could add. There are very few internet transactions that we can do that do not travel through more than one country, and because a great deal of the internet is hosted or serviced in some way in the

United States, that is why this piece of legislation is so powerful. It may well be that it is a UK individual sending to a friend an indecent image of a child, but because of the way that the internet works, it passes through the US. Depending on the extent to which the service providers are attentive and surveil these things, that is where it might get picked up.

Q43 Chair: IWF, you have been talking about content hosted on websites that people can access. You have just mentioned direct peer to peer. Is it possible to give us a rough estimate of what proportion is done peer to peer and what proportion is done through a website?

Peter Davies: Yes, it is. We do not share all the information we have or the means by which we acquire it, for reasons I am sure you will understand, but our estimation is that the highest volume of offenders is in the peer-to-peer category, which means they are not offending on the open internet. They are in groups of people whom they know, or think they know, and they have an increased level of trust and confidence that within those groups they can share child abuse imagery, child abuse material and so on. So the highest volume of offenders is in the peer-to-peer area.

There are offenders who use what is called the hidden internet, also known as Tor or The Onion Router or something similar. This is harder to penetrate, but I believe not impossible. These offenders are far fewer in number. The issue with them is they quite possibly pose the most serious risk because they are technically sophisticated and some of the harm that we see taking place in that part of the internet is some of the worst that we see.

Q44 Chair: And Tor, do I need a computer science degree to use it? I know you cannot find—

Peter Davies: Absolutely. I do not want to advertise it, but it is possible to download it and start using it on a normal home computer. It was designed by the US Navy in the 1980s, I believe, and released to the world. Some of our most sophisticated offenders use Tor. It is also important to realise that some other serious organised criminals use Tor as well. People may be aware of the arrest of somebody who was the proprietor of something called The Silk Road, so Tor is also used for drugs distribution, distribution of other criminal materials and obviously communication between criminal groups.

Q45 Steve Rotherham: IWF and CEOP have demonstrably been successful, if we have gone from a fairly high proportion of the images being generated in the UK to 1%. That in itself is a success rate. However, behind each of these individual images there is a victim. How successful are the police in pursuing the perpetrators of the crime against the child who has ended up on the internet?

Peter Davies: An excellent question, and I am not going to be able to provide a simple answer. As a centre and as a command, CEOP is getting more successful year by year in converting the intelligence that is derivable from the internet into outcomes in terms of safeguarding children. Last year we put out

15 October 2013 Susie Hargreaves and Peter Davies

more intelligence packages than ever to law enforcement and also to children's services in the UK, precisely with that intent. It is also important to highlight that within police forces there are very often technically proficient and committed online child protection units, so it is not as if CEOP is the only UK law enforcement asset in this area. The larger forces, particularly, often have real experts doing great work. I think we are in a transitional phase at the moment where we need to understand better what the overall capability and capacity is of the whole of UK law enforcement in order to tackle this kind of offending, and there is a plan in place to do that. We do not have the sufficiently high-quality robust data for me to give you proper arrest figures and things like that, and I can only really tell you at the moment that which gets reported back to CEOP. Again, there is a plan to improve and develop that because I think it is important for me, or the person sitting in my chair, to have a really good answer to that question and to be able to provide it for you. My observation is that there is a lot more law enforcement activity going on than it is possible to capture at the present time. This is something that HM Inspectorate of Constabulary has picked up on and noticed, and is working on.

John Carr has a way of putting things very simply and of course if there are 50,000 offenders out there and they are detectable, we should not really be resting until they have been detected. What we have to do in the face of a gap between provision and what we would like to do is prioritise, and that is what law enforcement and others charged with public safety always do. What we try to do is prioritise the people who do pose the highest risk to children by bringing in risk factors that help us identify them. We focus on the worst offenders—the people who are at the heart of networks that cause greater harm—so numbers are not the whole story; it is the seriousness and the numbers put together. The best evidence of whether we are arresting the right people of those that we can arrest is the number of children who are safeguarded as a consequence. I can tell you that in the annual report that we published in May this year, it was very clear that we are getting more successful than ever at doing the most important thing I think we can do, which is safeguarding children who are at serious risk.

Q46 Steve Rotheram: Is there any way that we can quantify that? While I absolutely accept the success of taking down images and the fact that it is demonstrably and obviously a criminal act to distribute the images, surely identifying the poor child—the individual who has been exploited—should be the primary concern.

Peter Davies: Absolutely, it is.

Q47 Steve Rotheram: Do you work with international law enforcement agencies? If we can identify an image that might not have been taken in the UK but might have been taken outside, do we still pursue that outside of our boundaries?

Peter Davies: Very much so, apologies. We have a victim identification unit in CEOP that has huge expertise in looking at images and looking for clues within them about how to track back to the child. This

was a specialist unit that was featured relatively recently on *Crimewatch*, for example.

We always seek to cultivate the best possible relationships with law enforcement partners in other countries. CEOP was a founding member, and is still a board and management member, of an organisation called the Virtual Global Taskforce, which now comprises eight different countries from around the world. Well below that strategic level, there are really good relationships, and indeed technically facilitated virtual private networks that enable, for example, my victim identification team to deal directly with colleagues around the world.

Some of our best successes have been quite remarkable regarding the speed with which we have received intelligence on UK activity from another country. We have seen opportunities to identify where that is taking place from the image and we have dealt effectively with the local police force concerned. There are occasions within my time at CEOP where that whole process from end to end has taken less than a day, and as a result children who were definitely at serious risk have been safeguarded and offenders arrested. That is the ideal. That is what we would like to happen every day. It is in the nature of the fluidity of these things and the complexity of international relationships that that does not always work, but it works sufficiently often to make us believe that it is worth pressing on with that. There is no occasion when we would not share information with law enforcement elsewhere that might give them the opportunity to do the right thing in their country as well.

Susie Hargreaves: We work also in the field of victim identification. We work very closely with CEOP; we are trained by CEOP. When our analysts see a new child, they look for particular clues within the picture and do some analysis of those new children. As a result, we also work very closely with international law enforcement—with Interpol; with Europol; with international locally-based law enforcement—and certainly through our work over the last three years, 12 children have been rescued. There are statistics that we can show in relation to rescuing children. It is about a partnership approach, but very much working very closely with law enforcement on an international level.

Q48 Steve Rotheram: Are there any changes that either organisation would like to see to either the law in this country or international law that would help you to do your jobs better?

Peter Davies: Yes. In terms of international law, we need to start from the point of recognition that the UK has just about the best suite of child protection legislation that there is, and that we are more of an example to others than we are in need of catching up. But when you are in the business of child protection, that gives you no cause for complacency, but it is important to note at a Committee such as this. There are two conventions, details of which I would rather supply separately, but they are the Budapest Convention and the Lanzarote Convention. One is mainly about online matters and one is about child protection. My sense is that if countries sign up to

15 October 2013 Susie Hargreaves and Peter Davies

and work up to both these conventions combined, that provides probably the highest straightforward level of assurance you can have that they will be equipping themselves to protect children online.

Turning to the UK, it is quite remarkable to me how far the criminal legislation, for example, around indecent images of children, which was, I believe, conceived and passed before the internet was around, has still pretty much stood up to the new world of child abuse online, and I do not think what we need is a basic root-and-branch piece of work. It is my firm operational view, and I have articulated it previously, that if there is one piece of legislation that would most help us tackle online child abuse, it would be the provision of a clear, consistent and properly enforced regime for retaining and accessing communications data, because we are regularly in a situation where we are unable to convert, for example, an IP address into a name and address for lack of that precise thing. I appreciate that it has been under consideration. I am merely repeating an operational view that I have articulated previously.

Q49 Chair: You can get a court order to get an ISP to divulge the address.

Peter Davies: It is possible. The issue is that it is not always an ISP; it can be a communication service provider. They are sometimes configured differently. My experience is that some are more able to provide the information we need than others, and when this legislation was under debate a little while ago, I took the view that our general attrition rate—the proportion of questions we would like an answer to that we do not get—is roughly 25%. Now, if you are dealing with a repeat victim or repeat offender, there are ways of getting around some of those, but it is implicit in that missing 25% that there will be lost opportunities for us to do the right thing. At the expense of sounding repetitive, I still think that is the most important single piece of legislation that would be of assistance to us.

Susie Hargreaves: Three things, if I may. One is that we do have some of the most robust legislation in the world in the field of child sexual abuse online, and certainly this is one of the reasons why we are setting up a back-office solution for countries without a hotline, because we will assess it under UK law and it means that it will be dealt with very thoroughly. So on that front, we do not feel that we need new legislation.

What we do feel though is that it is very important that people do not conflate the two issues between people accessing criminal content, which is what we deal with, and young people's access to adult content, and this is not particularly helpful. Certainly within Westminster, the issues need to be kept totally separate. Where, as a citizen and a mother, I might care that my teenager has access to adult content, it is entirely different to anybody having access to criminal content. We need to keep these very separate. We also need to have an awareness that we are a world model in relation to the internet industry support for the IWF, and in terms of the internet industry's commitment to support the removal of child sexual abuse content. They are currently working with us on a membership review to look at ways that they can step up that

support, and it is being done in a very positive frame of mind, and certainly it is one in which the industry does take its role very seriously. We only exist because of the industry.

The third thing I just wanted to say was that in relation to tackling this, it is our experience that young men aged between 18 and 25 are the most likely to stumble across it in the first place, and they will do that through the open internet, not through peer-to-peer networks. Because it is such a huge issue, we need to do much more to raise people's awareness to report and do the right thing, and to know that it is wrong. It is not just a question of looking at an image; it is a child who has been sexually abused. It is criminal. The consequences of looking at it are potentially extremely serious for everyone concerned, so it is to raise awareness to stop people going there in the first place.

Q50 Mr Sutcliffe: As a Home Office Minister in 2006, I visited CEOP under the leadership of Jim Gamble and, as you quite rightly said, Peter, it was set up as a unit because there seemed to be no consistency of approach across the 42 forces in relation to this issue. Seven years later, with all the experience that CEOP has gained, is the incorporation of CEOP into the National Crime Agency a good thing or a bad thing?

Peter Davies: I think it is absolutely a good thing. You will no doubt have followed our progress in the meantime and be aware that when I came in three years ago, it was very much a major issue. Since then, we have set about the business of contributing to the construction of the National Crime Agency, and also to making sure that we were absolutely able to dock into it effectively. There are a number of different aspects that I can offer up as evidence that it is a good thing, but the simple answer is, "Yes, absolutely no question." However, may I just offer one or two examples none the less?

Firstly, SOCA, and therefore CEOP, when you visited us, were never subject to a piece of legislation called the Children Act 2004, which places an obligation on public bodies—and others where appropriate—to have regard to the safeguarding and welfare of children in all their activities. Every police force was subject to that expectation, but not SOCA and therefore not CEOP. The new National Crime Agency has asked to be and is subject to that obligation, and I can tell you, as the Director of the CEOP command, that is influencing not just how we do the work that CEOP has traditionally done, but also influencing the way that the Agency thinks about the interests of children in its other activities, and that is quite a significant difference.

During the time I have been Chief Executive and now Director, the resources and the number of people available to do CEOP's work have increased, and that increase will continue into the NCA. There are aspects of what we have been doing in the past that are a major test of resilience, and the NCA is taking on some of those aspects in order precisely to help to take some of the load that that creates. The alternative is, as we have had to do in the past, that we have to move people from other parts of CEOP to support

15 October 2013 Susie Hargreaves and Peter Davies

some of these functions, which is not the best use of their time.

Another major gain is that it is not just about CEOP any more. Our mission is shared by the whole National Crime Agency and the structure of the agency is such that where the intelligence is sufficiently compelling and where the balance of risk dictates, the NCA can mobilise 2,000 of its own law enforcement officers to carry out operations to do with child sexual exploitation. One of the first tasks, other than set up the agency, that its Director General, Keith Bristow, was asked to do was to conduct a further investigation into child abuse at the Bryn Estyn children's home in north Wales, which was an operation carried out under the operational name Pallial, and there have been a number of releases of information and updates about that.

I could go on, but all those things point to the NCA being the right place for CEOP to be, and also to the major gain that it is not just about CEOP against the world—we are part of an agency that shares our objectives and ethos, and that is keen to help.

Q51 Mr Sutcliffe: I am heartened by that, because clearly it was a high-profile agency when it was set up, but what you are saying now is, with maturity, it is now back within the family, if you like. That then leads me on to the relationships with police forces in terms of whether CEOP just seen as, “You refer everything to CEOP,” or do forces actively deal with this as an issue in their parameters?

Peter Davies: I think forces have actively dealt with this for a long time. It has not always been fully acknowledged. I myself, before I came to CEOP, was involved in a major crime inquiry to do with a news group permitting the sharing of indecent images online, which we did in partnership with CEOP, but that was a local police force doing the right thing, and there is a fair bit of that going on.

Another aspect of the agency, which we have to approach with caution, is that ultimately it has a responsibility not just to manage how it uses its own 4,500 officers, but for making sure that the collective efforts of UK law enforcement deal with the risk in the most efficient and effective way possible. There is no big problem there, because we experience very good relationships with police forces. We co-operate very well, we try to find the right balance of resources so they can do what they do best and we can support them, or sometimes co-ordinate them—or very occasionally lead them, as appropriate. So the picture was never that bleak.

My experience, more anecdotal than out of certainty—refer to my previous answer—is that police forces are investing in the skills to do this area of work. Where I am less clear and less well able to answer with the accuracy I would like is on exactly how much capacity is invested in this across those 42 forces, the extent to which it looks similar and the extent that it can be interoperable, which means that officers from one force use the same systems and have the same approach as officers from another and can easily work together when possible. We have a plan for how we are going to learn that. The architecture of the NCA allows us to pursue that sense of national

consistency in a way we were never able to do before, and that is another significant gain.

Q52 Mr Sutcliffe: May I just follow that through because when I have briefings from our local police forces about what goes on within their force, it is about robberies or a variety of different things that are there, but this never gets reported, in the sense that they do not tell me about what work they are doing in this area. What I am slightly worried about is how we get—because a lot of this is about education and making sure that people understand the nature of this crime—the information out there? What are the mechanisms for raising the awareness of those forces to raise awareness within their communities?

Peter Davies: Yes. I think there is a whole variety of things. You may have seen when you visited CEOP that we have an education team and we have a very strong internet presence. We have a website to which the public are more than welcome to get advice and to access materials. We also have a network of ambassadors and volunteers, and we create new education packages every year with the intention that our ambassadors and volunteers can convey them to children. This is a real success story for CEOP, because out of a team of maybe three or four people, we manage to reach over 2.5 million children a year directly in a structured classroom or similar setting.

Our website regularly attracts more than a quarter of a million unique visitors per month and recently, when we did an information campaign about online child sexual exploitation, the number of people coming to our website was higher than it has ever been before. Of course, there is always a gap, and there are far more children out there who receive the message. This is one of the success stories, and we engage with any police force that wants to, in the same way as we engage with teachers or others to use the materials and take them out.

In terms of what police people talk about as their priorities, which is another aspect of what you were saying, I genuinely believe that child protection—online and offline—has never been closer to the mainstream of law enforcement in the UK than it is now. The police service has always been populated by experts—hugely passionate, committed people who make immense sacrifices to do the work that they do. But it is not just that. It is inescapable for police forces to have noticed the increased number of cases of what is called street grooming or localised grooming, another form of child sexual exploitation. There is a national policing plan in place to make sure every force has the proper capability and capacity to deal with that, and I am involved in overseeing the delivery of that, but that plan comes from Chief Constables and is being implemented by local Chief Constables, supported by their PCCs. This is an interesting area, because it is quite technically difficult and it requires a lot of innovation and flexibility and quite a lot of expertise to get. Generally speaking, law enforcement does not lack that, but keeping up with internet-enabled crime is always going to be a challenge.

I look forward to the day—I do not think it is far off—when police people talk just as much about the child sexual exploitation operations they are doing and what

15 October 2013 Susie Hargreaves and Peter Davies

a great result they had safeguarding children through an online inquiry as they would be talking about armed robbery and so on. Probably, in some police forces, we are already there.

Q53 Tracey Crouch: A lot of my questions have already been asked, but could I just ask: do you think that the social media providers could do more to help combat illegal behaviour?

Susie Hargreaves: I would say that all the internet industry regardless of social media—search engines, ISPs, mobile operators—are all extremely aware of their responsibilities in the field. We work very closely with all of them. Following the Secretary of State's summit earlier in the summer, we were asked to look at proactively seeking content in the future, which means we will be the first hotline in the world with the powers to do that, and that will mean we will need many more analysts. In order to support that, we have been working with the internet industry to look at ways that they will adjust their fees accordingly. We are in the middle of some very, very positive discussions and everybody has stepped up. In terms of their responsibility generally, I think all of them are really aware of what their responsibilities are and they are all doing what they can.

Certainly, I speak regularly at child online protection conferences and safety conferences, and you will have Facebook and Twitter there, and you will have those organisations talking about what they are doing to address the problem. I think they are aware—there are always things that all of us could do—of what they need to do and they are stepping up. But it is very much a group approach and a partnership approach, and in the same way as the police cannot solve it on their own and we cannot solve it on our own, we all have the responsibility to solve it. Facebook can do so much, but people also have to adjust their behaviour and so the education and awareness side is absolutely crucial—young people knowing how to protect themselves online. All these messages are really important, and that is part of our partnership in terms of the Safer Internet Centre with Childnet International, which goes out to schools and do all the awareness raising, and South West Grid for Learning, which gives support to professionals in terms of making sure that people can keep themselves safe. It is part of the overall picture, so I do not think it is enough just to say that one organisation needs to do more. Collectively, we all need to do more.

Q54 Tracey Crouch: Do you have support networks in place for your staff because this is pretty horrific stuff?

Susie Hargreaves: Yes, we do. We are currently recruiting for seven analysts, and we go through a very intensive recruitment process. We have a three-stage interview that culminates in them having a session where they see some of the images. We have quite a good dropout rate at that level. Anybody who sees any of our images has very intensive training. They cannot work on their own for six months—well, no one can ever work on their own, but they cannot take assessments without a second person looking at their work for six months. They have mandatory

monthly counselling, mandatory group counselling on a quarterly basis and an annual psychological assessment. So we do an awful lot on the welfare front, because obviously it is a real worry to us because they are looking at this content all day.

Of course, the public report to us stuff that is outside our remit and they still have to look at it. Sometimes they might look at something—they have to open a video to have a look at it—and it might be something very distressing, but is kind of outside of our remit, so that is the stuff that takes them by surprise. Yes, they are constantly seeing really very, very distressing stuff, but they are the most incredibly sane group of people and they do it because they are very committed to the issue. Certainly, when we rescue a child or we are involved in the rescue of a child, it is the greatest feeling in the world, and they do it because of their commitment. But we do protect them, yes.

Q55 Tracey Crouch: I assume it is the same at CEOP as well?

Peter Davies: Yes. I feel like saying, "What she said," but that is not quite adequate. We have a very similar approach. People are psychologically assessed before they start at CEOP, regardless of what job they are doing. That is refreshed on a basis that is proportionate to the level of exposure they have to material. It is really important that people have an exit strategy if it just becomes too much for them, and that is one of the huge virtues of CEOP being part of a larger organisation. People do not have to leave and find a new job; they can simply transfer to a different kind of duty, and that way they can move on and develop professionally, and continue to contribute in some other way to public safety.

We also have compared our provision with provision in similar law enforcement units around the world because—I am sure Susie would say the same—only absolutely the best is good enough in terms of taking care of our people. They do an exceptional job that most people would understandably shy away from, and we should be thankful that they are there to do it.

Susie Hargreaves: Absolutely.

Q56 Tracey Crouch: My very final question is probably relevant to you, Mr Davies. I have recently been doing quite a lot of work on modern-day slavery and saw quite a shocking statistic for someone who represents a south-eastern constituency: 49% of all instances of modern-day slavery are in the south-east. Are you able to give a figure as to perhaps what percentage or what proportion of modern-day slavery would be related to some sort of child sexual exploitation?

Peter Davies: I can give you a rough figure. Of course, as with all these things, it is based on that part of it that we can see, and while I may be getting it wrong by a few per cent, we would be looking at maybe 15% to 20% of human trafficking, which is probably our previous definition of what we now call modern-day slavery, to have a sexual exploitation element. Of course, some exploitation or slavery has more than one dimension to it and there is an overlap. We have dealt in the past with child trafficking cases.

15 October 2013 Susie Hargreaves and Peter Davies

There are other parts of the National Crime Agency, including the UK Human Trafficking Centre, which has a specific lead on that and is part of the Organised Crime Command, which is one of the other commands in the agency. More generally, our view is that we want to support those efforts precisely because the element of it that is child sexual exploitation is not the majority of it. There are a number of other factors to it: forced labour; street crime; organ harvesting; relationship abuse; domestic servitude. All those need to be taken into account, so the issue of modern-day slavery is something where we would like to support national efforts on it, but where we do not own it, and that is where I think it should be.

Q57 Tracey Crouch: So you would welcome the Government's intention, albeit it is very early days, of bringing in a piece of legislation that will help to give you those resources?

Peter Davies: I am not familiar with the proposed piece of legislation.

Tracey Crouch: Not yet, but it is an intention.

Peter Davies: From an operational point of view, I welcome the intention to take a very serious look at this issue and to do more, because within that thing that we call modern-day slavery are some of the most vulnerable people in this country, in desperate need of rescue—some will be children, some will not—by a law enforcement officer, not just a child protection person. Those people need help, so anything that puts the spotlight on that, and that challenges us to do better and do our best at that, is welcome to me.

Q58 Chair: Can I just ask you a couple of quick questions? Reference has been made to your comments about how you had identified 50,000 to 60,000 individuals but you just did not have the resources to arrest them all. Can you give us an indication of how far short your resources fall from being able to pursue all those leads?

Peter Davies: It is not just our resources; it is everything. This is an extremely large body of offenders and we have never been able to attach a number in which we had sufficient faith to that body of offenders before this year. I am told that there are a total of 85,000 prison places in the UK, and that gives you some indication of what would happen if we got up one morning and arrested all these people.

Q59 Chair: Is it at 5% or 10% you are able to—

Peter Davies: To be honest with you, I am really not able to tell you at the moment. One of the things we are doing as a command within the NCA, and obviously with the support of our colleagues in NCA and so on, is to identify how many of those people we can take on, but to have a plan for what we would do with the rest as well. Because I meant what John quoted me on, if I could, I would arrest all 50,000 of them, and I think that is what people would like. But it is not just about law enforcement capacity; it is technical capacity, the courts, the prison system and

the child protection system. None of this is resourced for a volume of offences of that nature, which means that we need a plan that goes beyond enforcement.

The truth is that for most high-volume or serious crime, you have to have a strategy that goes beyond enforcing it. You cannot enforce your way out of it, which is why our partnerships with the IWF and others, our work with industry to make the internet a tougher place to commit crime and our work with children to make sure they are less vulnerable to this kind of criminality all matters, because it is an issue for society as a whole and the solutions lie in lots of different places. Our contribution is to be absolutely focused in pursuing the worst of the worst—pursuing as many as possible within the obvious resource constraints that the whole of UK law enforcement has.

Q60 Chair: Can I just follow up your point about pursuing the worst of the worst? Susie Hargreaves rightly warned us to distinguish between material that is illegal and extreme and material that is not illegal but should be viewed only by adults. John Carr was suggesting that the police should be taking advantage of the Perrin judgment to pursue websites that are hosting adult content and taking insufficient measures to protect their content from being viewed by minors. That is a whole new area of operation. Would you have sympathy with the idea that the police should also be looking at that, or is your view that we should just concentrate on the really bad stuff?

Peter Davies: I do not think I entirely caught that part of his evidence. We have to prioritise. In law enforcement—in public protection—we have to prioritise every day. That is a simple fact of life. Anybody who suggests that you do not have to and that anybody has enough resources to do everything you would like to do is not unfortunately in the same world as the one I occupy. In terms of priorities, I would view the existence of child abuse imagery, with all the harms that it brings, and the existence of online child sexual exploitation, as a higher priority in terms of protecting the public than seeking to stop people who are below a certain age accessing things that we think are inappropriate for them. I make no apology for considering that as a priority. I am not entirely sure that John was suggesting that that is an area of work the police should get seriously into, but I was not here to hear his evidence.

I would certainly sympathise with the idea that given that it may not be something that law enforcement is necessarily able to prioritise, or that CEOP would prioritise, that somebody somewhere, if they are sufficiently concerned about that as a source of harm and have the ability to do something about it, should certainly do something about it. It may well be that age verification or active verification by the organisations that benefit from these people using their services is a way forward.

Chair: I think that is all we have. Can I thank the two of you very much for coming this morning?

Peter Davies: Thank you very much.

Tuesday 29 October 2013

Members present:

Mr John Whittingdale (Chair)

Mr Ben Bradshaw
Tracey Crouch
Philip Davies
Paul Farrelly

Mr John Leech
Steve Rotheram
Jim Sheridan
Mr Gerry Sutcliffe

Examination of Witness

Witness: **Stella Creasy** MP gave evidence.

Q61 Chair: Let us get straight in. This is the second session of the Committee's inquiry into online safety. We have three sessions this morning, and I would like to welcome for our first session Stella Creasy, the Member of Parliament for Walthamstow, Shadow Minister for Business. Stella, once you have your breath back, perhaps you would just like to begin by telling us your experience.

Stella Creasy: Sure. Can I start by thanking the Committee for inviting me to address you this morning? I come very much in a private capacity, as somebody who has experienced both the positive and the negative elements of online engagement.

I presume the Committee is familiar with what happened over the summer. A brief précis is this: I got involved in a campaign to keep female representation on bank notes—not a particularly big issue, but one that nevertheless we felt was important—led by a young lady called Caroline Criado-Perez. When that campaign was successful, we had a day where there was a lot of national press attention about it. Twenty-four hours later, Caroline contacted me to say that she was receiving threatening and abusive messages on Twitter. I contacted her to check that she was all right. She said that she felt she was. Twenty-four hours after that, she said, "Actually, I'm not okay". I then began reviewing the messages that she was getting and it was absolutely horrendous. She was getting 50 rape threats in an hour. It was an avalanche of abusive, very, very explicit, threatening messages from a wide range of accounts.

At that point, which was the Friday of that week—we had the campaign success on the Wednesday; by the Friday this was happening—I felt a duty of care to Caroline, having been involved in that campaign with her. I contacted the police that I had been working with in my shadow ministerial capacity when I was in the Home Affairs team to say, "Look, this is happening. We need to do something to protect this young lady". I was extremely worried because these people were trying to post up her home address and they were trying to find out personal information about Caroline.

We then also tried to contact Twitter to say, "Look, can you help?" I have to say, Twitter's response, of all the accounts that we could find for Twitter, was to block Caroline and then to claim that they were the victims of harassment. Twitter has since apologised for that and I think they recognise that that was a completely inappropriate response; that, when somebody was reaching out for help because they

were under that kind of attack, it was right for them to get support.

Over the course of that weekend, I continued to liaise with the police to try to identify the level of risk that Caroline was at, because the threats were relentless and escalating by that point, and also to try to hold the companies to account for their failure to act. Unfortunately, on the Sunday evening I then became a target for these people because I had spoken out publicly, both in the media and online, to say that I thought it was inappropriate. I then, along with a number of other women in the public eye, was subjected to the same sorts of threats over the course of the next two weeks. These threats were very graphic, very explicit.

I have always been a passionate defender of free speech. I also think you have to recognise that free speech comes when everybody feels that they can participate and the nature of these threats was that they were absolutely designed to intimidate, to harass, to close down Caroline and myself. They were very graphic, very specific. They were the sort of language that would be illegal offline and the argument that I made, and still make, is that there should be no distinction about this kind of behaviour. Indeed, one of the challenges we have here is to understand how what we have learnt about these sorts of activities offline can be translated into making sure that our online spaces are safe.

It continued for about a week and a half. There have now been a number of arrests. That case is ongoing, so I do not think it is appropriate for me to talk about that per se today, but I can tell you, from a personal perspective, however tough you think that you are, to get that kind of relentless onslaught—and I have had just a fraction of what Caroline has had, and Caroline is an amazingly brave young lady—is horrific. It is absolutely harassment. This is absolutely designed to intimidate, to scare, to frighten you, and it is absolutely an issue that we need to see that both the technology companies and the police understand is part of the modern world.

I think it is inevitable when you do this job that, while you might personally be affected by something, you feel, "What can we do to fix this?" You start looking at where the legislation can help and also where the culture needs to change to understand that, just because it is online, it is not somehow trivial. This is part and parcel of modern day life and indeed it is not Twitter or Facebook or Ask.fm that makes people say these things. It is something in these people that

29 October 2013 Stella Creasy MP

makes them say these things and so we need to be able to identify these people and engage with them and hold them to account for their behaviour because if we do not, the consequences could be quite severe. In many ways, it was an odd series of events because I had covered both the Data Communications Bill in my previous job and also the protection from harassment law and the stalking legislation. I felt both sides of the concern, which was why it was important what information the police could be asking of these companies and what possibly the risk could be to Caroline. The concern I had on that Friday night was, “Well, is this one person sending 50 rape threats, trying to find her home address, trying to target this woman, or is this 50 people?” We have to find a way. Just as offline, if you were in a pub, say, and it was one person who was persistently aggressively talking to somebody in that way, or 50 people, it would be a different type of risk. We do not have the capacity and the protocols in place as yet to identify those different ranges of risk and, therefore, there is a very real danger that we could miss something very serious as a result.

All the way through this, both as a politician and as somebody who was being affected by it, I had those two things in mind. We do not know what the risk is that we are facing and if people focus on the online element of it, they miss that fundamental question: what is the danger that we are trying to deal with here?

Q62 Chair: Were you able to get an answer to the question of how many people were involved in this?

Stella Creasy: No. As I say, there have been some arrests. It is an issue I have raised with the companies. The internet has come from the 4chan culture. We can have a long academic discourse about the gendered nature of that 4chan culture, but there is a very strong thread of concern that there should not be intervention in the internet, that what is wonderful about the internet is that it is creative. I absolutely agree. What that should not stop us doing is saying to the companies, “But, look, the way in which people are using these technologies is evolving and you yourselves say that you want to make sure they are safe spaces”. One of the arguments I have made to the companies is that they themselves could identify whether the same IP address was being used to send threats without having necessarily to pass that information on to the police.

If you recognise that there are different ranges of threats, if you stop thinking this is about online and offline, and start thinking that this is a range of offences that might be created—one of my bugbears about this is people kept trying to say this is about malicious communications and, therefore, the content of the messages being sent. I pushed back and said, “No, you need to understand this is about protection from harassment and the fact that these messages are being sent at all and the impact they are designed to have on the victim. Why does it matter whether it is 50 different people or one person?” If this person has said, “Please stop sending me messages”, and they continue to get these messages, that is harassment.

This concept of escalation—somebody who does not leave somebody alone because they are fixating on them, which we know very well from all the research into stalking and into domestic violence and intimate violence—we have not yet translated that understanding to online behaviour. We know that 50% of stalking cases involve online activity. To understand what was happening to Caroline and then to myself for those companies was not just a question of, “Is somebody sending a message that is malicious?” but, “Is their behaviour something that could be escalating?” They could, in the way that they have emergency protocols for dealing with reports of somebody who has gone missing, have emergency protocols where they do not necessarily have to share that data with the police, but they could themselves identify whether it is different people or the same accounts or the same IP address.

One of the things that we kept seeing was people taunting. They would get shut down. We know that Twitter was then monitoring my account and Caroline’s account, and Hadley Freeman and Catherine Mayer, other women who then proceeded to get these messages in that 10-day period. They were immediately suspending accounts, only for an account to open up two seconds later. I had a gentleman who was “killcreasynow”—I apologise for using these words at this time in the morning—“slutcreasynow”, “eatcreasynow”. He set up a whole series of accounts where he was targeting me with messages and taunting the police that they could not catch him because he could just set up new accounts. If you were the companies, you could identify whether that is different people all spinning off each other because they are caught up in this moment, or one person using the same IP address or even a very similar IP address to be able to say, “This is a different type of threat”.

Q63 Chair: Do you have any view as to whether there was a co-ordination taking place, that somebody was encouraging others to follow suit and send you similar messages?

Stella Creasy: No. That is interesting because, in terms of the actual messages that I would classify as relevant for the police, and I was always very clear that there were some I was reporting to the police, and there were some people I was just sending pictures of kittens to because they needed to calm down because they were being hysterical about the idea that somehow this was going to be the end of internet freedom if somebody did something about it. Within that there was a morass of people talking about the issue, because the wonderful thing about Twitter and all sorts of online channels is that we can communicate. Certainly there were people sending messages and badgering other people to get involved in the debate.

There were one or two accounts that were goading people to attack Caroline, certainly; whether those were the same people—Then, two-thirds of the way through, we came across a particularly nasty phenomenon, which was the faux friend. I had people sending me messages, going, “I think I know who is doing this to you and if you follow me I can send you

details of them. I am really trying to help you. Look, why are you ignoring me when I am trying to help you, save you from these people? Oh, look, Stella Creasy does not want to be helped. It is all about publicity. Oh, look, Caroline is not taking help”.

There is a wonderful academic called Claire Hardaker at Lancaster, who has just received some money—she was sat behind me—and who is just about to do some work on this about that element of behaviour. There was certainly an element of unconscious collaboration, I would argue, in that people identified it. Some people certainly felt it was sport to get involved in that debate and say, “You are obviously not tough enough. Can’t stand the heat, get out of the kitchen”, this kind of rubbish. There were other people who were seeing it as an opportunity to express what they thought was important about the internet, this concept that it is without boundaries. I would argue as someone who is a passionate defender of free speech that is a misunderstanding about the concept of free speech and how it operates.

There was no suggestion, as far as I am aware, that the people who have been arrested knew each other, but that is something, if this proceeds to trial, that perhaps might come out. Certainly you could see in some of the online communication the storm effect; that people get drawn into it and people become aware that you are responding to it. I think that is something people have noticed with trolling—that there is an element where people are trying to get people’s attention, what my mum used to call a professional wind-up merchant. I think that is slightly different from this behaviour, which was, “We want, in an aggressive, difficult fashion, to cause you pain, to cause you harassment”.

Certainly some people who were involved were enjoying the idea and, therefore, were drawn into it, because here was an opportunity to get pleasure from somebody else’s pain. Whether they had seen the conversations and, therefore, felt—sorry, I am not being very clear. There were the people who began it, then there were the people who got involved in it, and then the people who kept it going. I would say that there are probably three different groups in that and, within that, probably those latter two categories are people that you are talking about; who wanted to be co-ordinated by what was going on, but perhaps were not necessarily in touch with each other. I am not entirely sure. Maybe they were all direct messaging each other. I do not know. There was certainly that sense that they were being drawn into it by each other.

Q64 Tracey Crouch: Stella, you are high profile, prolific tweeter and obviously this level of abuse has gone too far. What sort of abuse have you been subjected to prior to this latest event?

Stella Creasy: What, by my mother or just in general?

Tracey Crouch: On Twitter.

Stella Creasy: We are all extremely conscious, I am sure, as all people around here who use Twitter and who are in public forums know, that you get a degree of banter, a degree of offensiveness, a degree of people trying to get a rise out of you. I respond robustly. I think I have had robust debates with a lot of people around this table as well. This is very, very

different. When I looked at what was happening to Caroline, it was very, very different. This was not people saying, “I disagree with you”, or even using colourful language to say they disagree with you or even just being trite and telling you that they think you are an idiot or using more colourful language to say that they think you are an idiot. These were very specific threats to do very, very graphic things that were repetitive; that were matched to, as I say, trying to identify someone’s address, trying to identify where you could find this person to carry it out. I got an email from one of these people, saying, “My accounts have all been suspended. If I apologise to you, can I have them back?” I looked at what this man had been sending and thought, “No, I’m just going to help the police make sure they have this information about you” because it was so different.

Prior to this, I have had one gentleman who, I would say, had edged on this sort of behaviour and indeed went after my mother, who was also on Twitter. That, for me, was an absolute red line, and prior to this summer he was the only person I had ever blocked. I think that is one of the things I really want to get across. As much as it is very easy in this debate to think this is about people not wanting to hear negative messages or not wanting to hear people disagree with them, for me there is a very clear divide. Prior to this summer, I had never blocked anybody, except for this gentleman who had been so utterly offensive to my mum, because I felt it was important to be open.

I felt, as much as it is sometimes unpleasant what some people might say to you, it was important to show that you are willing to debate and discuss and engage with people. A rape threat is not debate, discussion or engagement. A repeated rape threat or a repeated bomb threat, is not debate, discussion or engagement. It is designed to shut down and it is designed to intimidate, and we need to treat these things differently, just as we would in a pub. If someone came and said this stuff to you, you would draw a line between that sort of behaviour and banter and maybe someone being a bit off. You would make those clear distinctions.

Q65 Tracey Crouch: I have not had anything as similar to this experience as you, but I have had death threats and lots of abuse in that sense. Like yourself, I have never blocked anybody, but Twitter’s response to you from this was to just block people. Your response to that was that a rape threat is not a matter of bad manners. Do you think that Twitter were quick enough to respond to your concerns? Do you think they were helpful? Do you think they could have done more?

Stella Creasy: I think Twitter themselves would say they did not get it right. What is interesting, having spent some time now talking to them about these issues, is they are on a journey themselves about how different people in different countries are using their technology. I think they absolutely get that that weekend, where people were reaching out and saying, “Look, this is an attack”—the initial thing was, “Well, report abuse.” There was a lot made of an abuse button. If you are getting 50 rape threats an hour, it is not feasible to ask somebody to report every single

29 October 2013 Stella Creasy MP

message. That pressure alone on somebody, let alone the technology, even if it is reporting, “Here is another one, here is another one”, it is not feasible to do it. Twitter are on a journey of recognising that that is how people are using their platform, as are Facebook, as are Ask.fm; that these things are evolving and how people can use them to send those messages.

What I was very clear about is that if somebody is willing to say that stuff online, we should not treat it any differently from its being said offline, and if somebody is thinking in that way, there is potentially a problem because it is about this concept of escalation. The argument I had with both the police and the companies was not that it was for us to cope with this or to just block people. There was something about those people that needed to change. Therefore, we needed to be able to identify those people to work out whether they were on that path of escalation; that the kind of person who was trying to post up a young woman’s postal address so that she could be found obviously had some issues, and to simply say it was the responsibility of that young woman to keep herself safe, rather than to deal with the threat that this person posed, was not acceptable. You had to see it in the context of what we know about violence against women and what we know about that escalation process.

Q66 Tracey Crouch: You said there were 50 rape threats in an hour. That surely is an unusual event, or do you think this is commonplace behaviour on Twitter?

Stella Creasy: One of the other things I have asked the companies to do is publish their data about the numbers of reports of abuse they get and the numbers of the concerns so we can get a question of scale. I know that the Metropolitan Police over the summer have said, since this all happened, they had had an increase of 1,500 reports from people about this. I welcome that because I think we have to recognise the scale of what is going on and, therefore, the potential risk. Talk to Women’s Aid or talk to Refuge about the numbers of people they might deal with who have been victims of violent assault or victims of a former partner who is using this technology to commit the crime, who is using it to continue to harass people. I think to see that as somehow separate, or not to have ways of identifying if somebody is using online forums to harass and to continue a programme of harassment misses a trick, because we would not let that go offline. Women are subjected to a particular type of misogyny online and I think that comes from that culture of the internet. That has to change as women come online and I do think that will change. What I would say is that, as much as these technologies have these problems, there are also great opportunities to redress some of that and to have a public debate about these issues.

There are also other victims of this behaviour. We do not know the scale of how people are using these technologies. My point is that it is not the technology; it is the person underneath it we have to get to grips with. If the technology allows us to identify that person, that is a positive move to me because it allows us to intervene at a much earlier stage. When you look

back at some of the histories of people who have been victims of intimate violence, you can see points where they have had this behaviour and everyone has said, “Well, just don’t go on Facebook” or “Don’t go on Twitter”. Leaving aside their own personal freedoms, that is a missed opportunity to understand that the risk to that person is escalating.

Q67 Mr Leech: I do not think any reasonable person could try to justify the sort of abuse that you and others have received in this case. It has clearly stepped over a line, but there is also a very grey area on social networking about what one person might think is overstepping the line and what others do not. I suppose my question is, how do we come to a conclusion about what is acceptable and what is not? How much of it is important for us to make sure what we are doing online is very much on the right side of the line, rather than the wrong side of the line, to set a good example?

Stella Creasy: Could I just flip that back to you, John? You said there is a grey area online. Do you think there is a grey area offline?

Mr Leech: Yes, I do, absolutely.

Stella Creasy: That is exactly the point. It is not that the online world is somehow different or separate or distinct in terms of these questions about what is offensive speech or what is a threat. We have laws and we have guidance that the CPS and the police are supposed to use offline. That we do not necessarily think about how we can apply them online is the challenge here, not that those debates do not exist offline as well.

Q68 Mr Leech: Is it not the case, though, that more people are prepared to overstep the line online, rather than offline, because they feel a lot braver behind their computer, rather than face-to-face with someone?

Stella Creasy: I think that is absolutely true. That does not negate the point that this concept of a grey area is not distinct to the online world. I do not think we should be drawing distinctions between online and offline behaviour. I think we should be trying to understand how people are using different forums, whether in person—I have had poison pen letters; I am sure other members of the Committee have as well—or whether online people are sending these messages. There is a risk that we trivialise something. One in five people in the world are on Twitter. That is only going to grow.

This is not a separate, distinct world in which we have to make up new rules. We have to make this work in reality, in the messy reality, of the lives we live. You are absolutely right that anonymity makes it easier to be offensive to somebody, easier to threaten somebody. Someone threatening to rape you or to put a bomb under your house or posting up your address, or coming around to your house, is as threatening and as intimidating online or offline.

Q69 Mr Leech: Do you not think, though, when people stretch boundaries online, it then encourages some people who do not recognise boundaries to overstep the line?

29 October 2013 Stella Creasy MP

Stella Creasy: I agree, but I do not think that is to do with being online. I think that is part of modern culture. That is why we have guidance and we need to make sure that we are able to understand the risk that people might face and also to be robust about defending the right to be offended. We have also recently changed the laws around the right to be offended, haven't we? That will apply online as well. We should not let the technology get in the way of saying these are live debates in our society. What people will say to each other in any different context could be offensive or could be designed to intimidate and we need a protocol and way of understanding what that is.

Q70 Mr Leech: Changing the subject slightly, you said earlier that it was not clear whether it was one person making 50 threats or 50 people making one threat. Do you think there is a problem with the systems that the likes of Twitter or other social media sites have in place, that they cannot necessarily distinguish between whether it is one person with 50 threats or 50 people with one threat?

Stella Creasy: No, I think it is perfectly technically possible to do that. Justin Bieber gets millions of tweets a day. You would expect that account to get a lot of traffic. I have talked to Twitter about the concept of an online panic button. Because of this, I have now had a panic button installed in my house. I have a button that if I feel in distress, I can press and the police know, because of the history of what has gone on, that possibly my property might be at risk and, therefore, to come around. Online, if you say, "I am being attacked", and your account is getting a high level of traffic compared with what you might expect it to get—so say the numbers of followers you have or the number of people you follow, or the type of language being used—those algorithms are not particularly difficult to put in place. You have to have the culture as a company that says, "We need to be scanning. We need to be looking for that".

One of the things I have tried to follow up with Twitter is obviously if they are going to have an abuse button and there is every concern, rightly, that people might then—in fact, quite a few of the people on Twitter said, "Right, we are going to tag everything you tweet as an abusive message to see how you like it". But if people are going to use these technologies, what do you do with the information? They hold an awful lot of information about people already, in terms of the account that you set up, where it was set up, what kind of messages it is sending, for them to be able to do that kind of analysis; to be able to say, "There is a distinction between the Justin Bieber account, which we expect to get millions of tweets a day, and what suddenly is happening here. Is that a cause for further investigation?" If my property was getting a lot of reports, the police might flag it up and go, "Hang on a minute, we might need to investigate this a bit further". An online panic button system would allow someone to say, "Look, this is a problem", and for Twitter to say, "Oh, you seem to be getting a lot of information here. Yes, maybe there is something going on. Can we help you?"

Q71 Mr Leech: But my question was not about whether it was technologically possible. It was whether Twitter and others were using the technology to its full potential and whether you think there are other things that they could be doing to make that—

Stella Creasy: The equivalent of an online panic button is absolutely something I have discussed with Twitter. I would like to see other technology companies having it. The answer to your question is no. As far as I am aware, none of them do this at the moment, although I think they are all thinking about it because this is an evolving debate, particularly in the UK, about how people are using these technologies.

Still now somebody sends me an abusive message that crosses that line. I still get one or two of these. Those accounts get suspended very quickly. That process of a kind of online temporary restraining order, essentially, seems to me to be something that these companies can explore, again if they have protocols in place. One of the things I am concerned about is for that not to be abused. In order for that not to be abused, there needs to be a protocol for it. None of these companies have this in place at the moment. I think they are all starting to look at it because of this public debate.

Q72 Mr Leech: Why do you think they have been so reluctant to put these sorts of things in place? Is it just because of an attitude about free speech or is it more about the cost?

Stella Creasy: I think we have all seen these issues as issues around malicious communications, rather than understanding that there could be other forms of behaviour at stake here. How you would then act and how you then, as a company, would abide by local laws, as they all say they would, is very, very different. If you are only being asked to deal with one type of offence, which is malicious communications, then you need a protocol to be able to look at the communication and decide whether it is malicious. If you are being asked to deal with a harassment case where somebody might be sending the most innocuous messages, but it is the contact and it is the fact that somebody is continuing to contact somebody, continuing to set up accounts, continuing to pursue somebody that is the problem, that is a very different type of issue.

I do not think these companies have even begun to scratch the surface of how their technologies are being used to commit those sorts of offences and so what they might be able to do to help protect their users to make it a safe space. The question for all of us as public policymakers is, can we get them to have that conversation and do it in a way that is fair and proportionate so that we do not close down the internet; we open it up for more people because it will be a safer space for more people?

Q73 Steve Rotheram: There is not a country in the world where freedom of speech is absolute. Before we get those people perhaps who are listening or reading the transcript claiming that somehow we are trying to close down freedom of speech, let me say it is absolutely not the case, and, in fact, as you just

29 October 2013 Stella Creasy MP

mentioned, we are trying to defend freedom of speech and encourage more people to take part in the likes of Twitter debates and stuff. You spoke earlier about your personal experiences of being a victim of harassment on Twitter. In your view, are the laws to tackle harassment fit for purpose in the online world?

Stella Creasy: Thank you, Steve, and I just want to pay tribute to the work I know you have been doing about trolling as well, because it was you and I who first started, well before this ever happened to me, and I never ever thought I would need to know quite as intimately and directly what the law would be. I think the honest answer is we do not know. Obviously the protection from harassment law was updated about a year ago. We have seen the first initial statistics about it. That is not just about online behaviour. I think there is a way to go for matching that understanding of what forms of behaviour online are similar to behaviour offline and, therefore, potentially problematic for our police and for the technology companies. I think we have to press to do that because one of my concerns is, from a public value-for-money perspective, the sooner we identify these challenges, the sooner we can get the right training in and the sooner we can prevent some of the crimes that might end up being very, very costly. There is a real value in getting everybody up to speed in the way in which these technologies can be used.

I think the Protection from Harassment Act has a way to go in terms of its application. There are concerns for me about the 4A, 4B—I apologise to the Committee if that is too technical—about how it can be implemented. We have to see. The initial figures look a bit mixed about whether that has been used to truly tackle these problems. I think we have legislation at the moment, but we do not necessarily have the culture at a local level to be able to put it into practice. Certainly I found, when I was trying to get the police to engage in this debate, that I kept getting put through to the person who held the Twitter account for a particular part of the police rather than somebody who could understand that on a Friday evening there was potentially a young girl whose address could be on the web and she could be the target of all sorts of malicious behaviour.

That is not about having separate departments or separate specialist people when this is so much a part of everyday life. You want your police to know the rules of the road. You want your police to know how the internet is being used and to be able to understand it, because that is what they are going to have to police.

Q74 Steve Rotheram: Do you believe it is a problem with shortcomings, in effect, of enforcement, rather than in the legislation itself?

Stella Creasy: I think we will not know whether the legislation matches what we need to be able to deal with until we have more enforcement of it. It is just too early to tell. I think there is a wider point about understanding both the concept of escalation, the concept of harassment, and then how that might happen online as well as offline and what you can do about it, and what you can ask companies to do about it already. What I would say is that, since the summer,

I have noticed the police are willing to engage with those threats. They need help. I think that is why we have talked about having cyber specialists coming into the police, because this is about a set of skills matching a cultural change.

Q75 Steve Rotheram: You mentioned Claire Hardaker earlier, who is doing some fantastic work on looking at perhaps the reasons behind why the culture is so different online and offline. Just to broaden that out a bit, are there any changes to legislation you would like to see to combat harmful or illegal content on the internet, and not just in the social media field?

Stella Creasy: From a personal perspective, I think some of this is about the CPS and how they respond to the powers that they have. I would like to see the CPS being very proactive about drawing distinctions and defending that right to be offended, that right for people to be close to the bone—what is lovely about British culture is that we have that stream of quite out-there comedy, out-there satire and out-there debate and discussion—and, in order to defend that, saying, “Here is the stuff that crosses the line. Here is the stuff that we have to be clear is unacceptable, is illegal. It is illegal offline. It should be dealt with the same way online and we will act on that to make sure that we draw that boundary”, so that we can have all the lovely banter, the jokes, the debate, the discussion and the humour that is so much part of British culture.

It is genuinely difficult for me to tell on a personal level, until we have seen this case through, whether the law matches that standard. The messages that Caroline has received, for me, certainly breach that level. I would want to see action and I want to see the people who sent those messages being held to account because I have seen the damage that it has done. I have seen how affected she has been personally by it and that is what those people were trying to do, and that is an offence. It is an offence offline and it should be an offence online.

Q76 Steve Rotheram: I agree with that critique of current legislation. I am beginning to believe perhaps there is slightly too much in regard to things falling between the cracks. I have identified at least seven different Acts of Parliament that can be used in the online world for those people who are trolls or who do these despicable acts. Obviously all that legislation was before Facebook and Twitter and there is no mention of trolling. It is not identified. The word “troll” is not even identified in the legislation. Perhaps what it needs is just a clarification, rather than a reworking of any of the laws we currently have.

Stella Creasy: Yes. I have been repetitive with the Committee about this. I do not want to draw a distinction between online and offline because that makes it somehow mean that, if these people were doing it offline, it would be easier to do something about it than online. That is just about ease of access to them, rather than necessarily the technology. We have laws. If they are not necessarily being applied, we have to work out what it is about the way in which the online world operates that makes it harder for people to see the connections between those things. I am also resolute that it is not for those people using

29 October 2013 Stella Creasy MP

the internet, like Caroline, to cope with this pressure. It is for us to find a way of helping to bridge that gap and change the debate on it.

Q77 Mr Bradshaw: Do you know how many arrests there have been?

Stella Creasy: I believe there have been five arrests.

Mr Bradshaw: Do you expect there to be prosecutions?

Stella Creasy: On a personal level I think the case is there, but it is for the police and the CPS to make that decision. I absolutely respect that. The evidence and the behaviour seems to me to fit everything I have ever seen but, again, I am the victim here in that sense and so it is not for me to make that judgment call.

Mr Bradshaw: But you agree that an important part of the law is to act as a deterrent and that prosecutions could act as a deterrent in this case?

Stella Creasy: Prosecutions would be about holding people to account for their behaviour. I do not think there is any disagreement about this, that that kind of behaviour over the summer was absolutely horrific, was completely illegal. The question for all of us is whether we are able to meet the test to make an effective prosecution.

Q78 Mr Bradshaw: What this case seems to have exposed to me, which is very depressing, is an underlying current of violent misogyny that is still there in society. The way you deal with expressions of this is, in other media, through the law. It is not an exact parallel, but I suspect that people are now much more careful about what they say about other people following the action against the Speaker's wife, for example. We are learning how to use Twitter. What I am saying to you is I hope what this case achieves is a change and that is what I am looking to see: whether you are optimistic, whether this could act as a positive change.

Stella Creasy: I have great optimism about the future being more equal online and offline, because one of the things these technologies and communications do is allow us to have those debates. It is like the No More Page 3 campaign. It has been entirely run online and that has opened up a space to say, "The impact of seeing these images on women is X and this voice needs to be heard". We would not have had the capacity to communicate in that mass way before. As much as, yes, prosecutions can act as a deterrent, I also think what has been positive is that there has been a broader debate that says, "This is completely unacceptable".

I found it very striking that, in retweeting the messages that I considered to be illegal, quite a lot of people said, "I had no idea this was happening"; in the same way that the EverydaySexism Twitter account and all that campaign—again, which is all online—has allowed people to see a side of society and to see some of that misogyny that people had never really engaged with or become aware of. I would love to think that a prosecution would be—and I do not think addressing misogyny, addressing inequality, is going to take that cultural debate. What is fantastic about these technologies and why I am so passionate about making sure we have free speech is

that they allow a vehicle for some of that change to take place as well.

Q79 Jim Sheridan: Stella, many, if not all of us, are discovering the nature of our job attracts through social media and emails some of the unsavoury characters in the world.

Stella Creasy: Yes, I am sorry about that. My mum just gets bored. She sends emails. I have told her.

Jim Sheridan: Does she send them to me?

Stella Creasy: I would rather she was sending them to you than me, I tell you; some of the things she tells me.

Jim Sheridan: No, but seriously, as I say, we do attract so many nutcases in the country, but what you have described goes way beyond anything that should be allowed. Just in terms of legislation and to follow on from Steve's point, the 2008 Criminal Justice and Immigration Act, it sounds to me—this was before social media kicked off—that it is something we could revisit and look at again and the value of it, if indeed that is still working. The main question I am asking is about the international scene; for instance, in countries where this kind of behaviour may be legal. What can we do to stop it coming from countries that might find this sort of behaviour acceptable?

Stella Creasy: I have no reason to believe that any of the people sending messages to myself or Caroline or indeed any of the other figures over the summer were from anywhere other than the UK and, indeed, all the prosecutions have been in the UK. One of the suggestions that one of the reasons why we can't bridge that gap between what our law does offline and online is the global nature of the internet. I do not necessarily think that is the case. For these technology companies, the awareness of how people are using their tools to create crime is an interesting question because that then could apply to other jurisdictions in terms of if you were to see escalating behaviour. It is interesting. The woman who is in charge of online safety at Twitter comes from a domestic violence background and said to me, "Oh, yes, I totally get the point you are making", and you are thinking, "Okay, so why don't you have the systems in place to then be able to address this?"

I think we have to be wary of the idea that, because the internet is global, there can be no local response or no local engagement on any of these issues. Nothing has disproved that to me so far. We also have to be very careful and one of the things that is so important about the internet remaining a space where people can have freedom and anonymity is that it has also been a force for good in terms of human rights issues. It has been a force for good in terms of giving a space for people speak freely, where they are not given freedom in their own countries.

We have asked Twitter to make it clearer that harassment was not acceptable in their guidelines. That cuts across all their jurisdictions. At that point, Toby Young accused me of being like a Chinese dictator for suggesting that harassment should not happen online. I wanted to point out to him that this was already illegal in this country. What is harassment may well be in the eye of the beholder in some countries and, therefore, it is about the systems that

29 October 2013 Stella Creasy MP

these companies have to assess the complaints that they get, which is why we need to see the scale of the complaints. In the UK they say they comply with local laws. We have the Protection from Harassment Act. The question is, how are they then using that information to be able to make sure that they are responding to any concerns that are raised with them? They have a way to go yet. So do a lot of companies. That Twitter are engaging in this debate for me is very welcome. I would like to see that then develop.

Q80 Jim Sheridan: If you are receiving horrific emails or tweets or whatever it may be, for me it does not matter where it comes from. Do you think there is anything more that the providers can do to stop this in a global market?

Stella Creasy: As I say, what is interesting is whether it is happening in other countries and I think there are cultural variations in how people are using these technologies around the world. These companies are also growing. Twitter did not exist five or six years ago, so it is growing as an organisation to have the capacity to deal with it. They now have a new team of people looking at online safety. I would expect them to take the lessons they are learning from the UK and think about whether they can be applied to any form of behaviour on their platform around the world. That will be a question for Twitter. It would be a good question if you guys are speaking to them about it. What we have to focus on is how we keep our systems safe in the UK. How do we make sure that every system in the UK has the freedoms that we want them to have, online and offline? How do we make sure, when we get instances like this, that our own local laws are being used to best effect to open up that space?

Q81 Philip Davies: I would like to think of myself as a great champion of free speech, but clearly what you and Caroline and others have faced is beyond what anybody would hopefully think was acceptable. I just wondered whether you felt, given the scale of Twitter and the pressures on, for example, the police, this is something that is just going to be in many respects unsolvable through the normal course of the law in the sense that, if Twitter is already at the extent it is and is going to grow further and police resources are so stretched, is it going to be the case that the police, even with the best will in the world, will simply not have the resources to be able to pursue all these particular cases?

Stella Creasy: I appreciate what you are saying, Philip, about recognising that this is about the freedom of speech of people like myself and Caroline to not be subjected to this kind of behaviour.

Philip Davies: Absolutely, yes.

Stella Creasy: I think the question for all of us is, what does that behaviour embody? The person who uses this platform to repetitively send those kind of messages—what else might they escalate to do? How else is this connected to other forms of crime? That is the way to look at it, which is not to say that somehow there is something unique about online behaviours but to ask where they interact with offline behaviours. When you do that and, as I say, when you look at

some of the cases around stalking and harassment and you see people getting messages online and people saying, “Well, just don’t go on to Facebook” or “Don’t use these forums”, rather than recognising that the person who is sending those messages is fixating on somebody, could then become an even more severe risk to that person, and the sooner we intervene, the sooner we might be able to address that person’s behaviour, prevent in the future much more damaging and indeed more expensive and resource-intensive crime from taking place.

Keeping people safe—there is a gender issue in this and it is disproportionately women who face these challenges—will be both better for the public purse and receive better outcomes. I understand the concern about resources. What I am saying is that the online world is an opening to seeing and identifying crime and detecting it quicker. We should see that as an opportunity both to save money and get better outcomes, rather than another set of issues to deal with.

The other example from this for me was that the EDL were using Twitter and Facebook to organise coming to cause problems in Walthamstow. There was a time-lag between the police understanding that, seeing that information and engaging with it—in the same way during the riots we saw a time-lag between the police engaging and interacting with that information—to be able to then use the online world to detect and prevent crime. There is a big value-for-money argument about how, if you understand that is how people are using these technologies and you have a way of dealing with them, you can get things at source in a way that if you wait until much later on, they will become much more expensive. We are nowhere near there yet, and in fact what people are trying to say to me is, “Well, don’t we need specialist units?” which to me is a bit like saying, “Don’t the police need a specialist unit for dealing with the telephone?” This is so much a part of everyday life, we need our police to be able to use their own personal experience of it to understand how it might then lead on to further crime.

Philip Davies: Obviously I am delighted that there have been some arrests and I hope there will be prosecutions and convictions and, like Ben Bradshaw, I hope that that will act as a deterrent so that people realise that they can’t get away with this. Hopefully that will be the case. I just wondered whether, when you have received these threats and people like Caroline have received these threats, which must be horrendous, you felt—and do you know whether Caroline felt—that they were genuine threats in terms of people were intending to carry out these things that they were saying or whether they were just unacceptable abuse?

Stella Creasy: I think if someone is trying to post up your home address, Philip, that is pretty frightening and that is very, very distressing to somebody. To then receive continued threats, continued aggression, continued details about what someone is going to do—these people went into tremendous detail about what they might do to my dead body once they had killed me and once they had done horrible things to me and how they might do it again. I defy anybody not to find that deeply threatening, deeply unpleasant.

29 October 2013 Stella Creasy MP

This is the thing about the Protection from Harassment Act. It is not about the content. It is about the impact on the person. Nobody can be unaffected by receiving that kind of avalanche of threatening behaviour over a persistent period of time, to not think, "Actually, is that person outside, who I don't know, the person who has been sending those messages?" The thing about the anonymity of the internet is that it could be anybody sending those types of messages to you. It becomes even more distressing in a way, because you do not know who it is who feels the need to send you that sort of message.

Q82 Philip Davies: No, I do not disagree with any of it. I am simply playing devil's advocate. I am trying to think about some of the defences that some of the internet social media sites might give. I was just anticipating what you thought if they were to argue that, if there are these people out there and they are serious about these threats, it is better for the law enforcement agencies that they are out there in public so they are able to be traced, rather than to be still there but untraceable and unknown; that in some respects it would be easier for the law authorities to deal with these people, if they are serious about doing this thing, if it is up there for them to trace.

Stella Creasy: We should use people as bait to draw these people out?

Philip Davies: I am merely asking for your response to what may be a line of defence that these social media companies give.

Stella Creasy: Here is the thing, Philip. Surely what matters here is the victim. The victim was Caroline and her life was dramatically changed by the behaviour of these people. Our job is to make sure that nobody's life should be curtailed and nobody's free speech should be curtailed by the behaviour of these people; that it is not for Caroline to cope because "at least we know who these people are", as a containment strategy. It is for us to say both in law and in culture, "This has to change, because it is not part of the society we want to live in".

Philip Davies: No, I agree. I was not giving you my opinion. I was trying to pre-empt what people might say.

Chair: I think we had better call a halt at this point. We have another two panels. Stella, can I thank you very much for coming?

Stella Creasy: Yes, and can I just thank the Committee for looking into this? I think it is difficult to get right, but it is welcome that you guys are looking at how you could get it right and how you could support both the police and the technology companies to work with us.

Chair: Thank you.

Examination of Witness

Witnesses: **Nicholas Lansman**, Secretary General, Internet Services Providers' Association, **Dido Harding**, Chief Executive Officer, TalkTalk Group, and **Hamish Macleod**, Chair, Mobile Broadband Group, gave evidence.

Q83 Chair: For our second session, can I welcome Dido Harding, the Chief Executive of TalkTalk Group, Hamish Macleod, the Chair of the Mobile Broadband Group, and Nicholas Lansman, Secretary General of the Internet Services Providers' Association, and invite Gerry Sutcliffe to start off?

Mr Sutcliffe: The topic of our inquiry is online safety and, notwithstanding the evidence we have just received, we recognise we are talking about a growing situation here, not a closing down, and that is not our intention. Clearly there are responsibilities and there are issues that flow from that in terms of what needs to happen. It would be interesting to hear, right from the start, what you do already to prevent access to harmful or illegal material online; just a general flavour of what it is about at the moment. Whoever wants to start off.

Nicholas Lansman: Shall I kick off with some general points?

Mr Sutcliffe: Yes.

Nicholas Lansman: First, you have to treat illegal material very separately from legal, which might be age-appropriate. With illegal material, right across the industry, whether mobile or internet, have done a lot of work over many years here, primarily setting up the Internet Watch Foundation in 1996, and illegal material is dealt with in a variety of ways. The priority is to remove illegal material from the source. In the UK we now have much less than 1% of illegal

material that is hosted in the UK. Secondly, to try to remove it even when it is abroad and, thirdly, to create, with the IWF, a blocking list so that ISPs can block illegal material before people can stumble across it. That is illegal material and what I mean by that is child abuse material, but also terrorist material. I think the industry has been extremely effective in dealing with that side of things.

In terms of age-appropriate material, there have been huge developments more recently and I will allow Dido to contribute to that discussion. Principally, there have been developments in terms of creating an active choice for customers when they purchase broadband to make that decision of whether they want to engage filtering. Filtering is now going to be provided for free and a whole-home solution. It is very important that it applies to all devices in the home, whether it is PCs, laptops, tablets or indeed smartphones. Those filtering technologies will be easy to use.

Q84 Mr Sutcliffe: Easy to use, but is there not an education and development process to go alongside that? It is all right having the technology to deal with it, but how do you encourage people to be active?

Nicholas Lansman: That is a very good point. Technology alone is not the only solution and education and awareness is fundamental to the process. ISPs over many years have provided material on websites, on leaflets. They have also been visiting

29 October 2013 Nicholas Lansman, Dido Harding and Hamish Macleod

schools to educate teachers and parents. There is also the UK Council for Child Internet Safety. We also have Safer Internet Day. A great deal is being done to educate. Still more needs to be done and this is about creating the tools to ensure that parents become confident with the use of the internet and that they can also communicate that and have that dialogue with their own children.

Dido Harding: I have said a number of times that I think internet safety is the road safety of our generation. When I was a child, my parents were advertised that with Clunk Click. We had the Green Cross Code. Seatbelts were just being rolled out into cars. The airbag had not yet been invented. You had a whole load of technology innovation, public awareness and education in schools. I can remember the Green Cross man coming to my school. Internet safety is as broad an issue, if not broader, than road safety for our generation. There is a lot that is happening on the technology front. There is a lot that is starting. We in TalkTalk have lobbied heavily to see internet safety in the primary curriculum and we are delighted to see that it will be coming in. There is a lot that needs to happen in education and public awareness. There is not one single bullet. We all have a role to play in making sure that the digital world is safer than it is today.

Q85 Mr Sutcliffe: I like the analogy of the road safety because I think you are right, but part of the problem that we have, in terms of the evidence and in our own lives, is that parents do not go in to watch what the kids are watching online and things like that. The analogy about if a child had a TV set in the bedroom, years gone by, there would be an issue about what they were watching. What is concerning me is that the technology is there, but there is not the cultural change in terms of parents being able to understand what they need to be doing.

Dido Harding: Nicholas mentions filtering. At TalkTalk we have had a whole-home filtering product called HomeSafe available now for just under 2.5 years. We have about 1.2 million of our 4 million customers use it and 400,000 customers have activated the Kids Safe element of that, choosing to block certain content in their home. Just as you say, we have learnt that it is important to keep it simple because most of us find the technology baffling. You do have to have something that covers the whole home and you also have to work hard, and all four of the major ISPs have committed to work on a public awareness campaign, because all of us are learning how to use this. It is not just enough as an ISP to provide the gadget. You have to help people understand how they might use it. The most valuable thing you can do as a parent with young children, and I say this as one, is talk to your children about what they do online. If you don't engage with what they are doing online, no technology is going to help them.

Mr Sutcliffe: I think that is spot-on.

Hamish Macleod: Can I just make a mobile contribution? As far as the Internet Watch Foundation and the illegal side of things goes, our approach is very similar to the fixed ISPs. We take the list. It gets updated twice a day and any attempt to access sites

on the illegal list will be frustrated. As far as the age-inappropriate content is concerned, people first started to use the mobile to access the internet about eight or nine years ago. At that time we published a code of practice and part of the code was that we offered a filter for the internet browsing service on the mobile. For all prepaid phones, though, the filter was put in by default. For most contract phones it was also put on by default and in the next 12 months for all contract phones it will be put on by default.

Mr Sutcliffe: The filters will be basically free? They will come as standard?

Hamish Macleod: Absolutely, there is no charge for them.

Q86 Mr Sutcliffe: Is there a need for consistency of approach across the range of providers and is that happening?

Hamish Macleod: The approach we have taken on the mobile is that, when we first published the code back in 2004, we appointed a body called the Independent Mobile Classification Body to achieve this level of consistency. It was a subsidiary of the premium rate regulator, who was called ICSTIS at the time. The reason for that was that most of the content about which there might have been some concern was premium rate adult content, so it made sense to work hand in hand with the premium rate regulator. We carried out a review of that earlier this year and, as a result of that review, we have appointed the British Board of Film Classification as our independent body who give us editorial advice as to how we should calibrate the filters.

Q87 Mr Sutcliffe: What are the linkages like with law enforcement agencies and trying to help them with the speed of the technological changes that are taking place? Do you think that is working well or could more be done?

Nicholas Lansman: I think it is working very well. There is a long-standing process in place where, according to the regulations, ISPs will be approached by law enforcement to hand over data and that is done. It seems to work well and we know that, in a variety of cases, law enforcement have taken and followed those investigations and will make prosecutions where people are behaving illegally online.

Hamish Macleod: Can I make one point on that, though? A few months ago there was a summit held with the major ISPs and mobile companies about the work of the Internet Watch Foundation and whether they should be more proactive in seeking out illegal images on the internet because, up to that point, the memorandum of understanding specifically with the CPS was that you could only respond to public reports and then you could go and look for the stuff. Now we are moving to a point where they will go out and look for the stuff. That should be more efficient because, of the level of public reports coming in, only about one in 10 of them are illegal. That should be more efficient and should lead to fewer public reports, we hope, because they are getting to the content before the public does.

However, the IWF is part of a safeguarding ecosystem. They are not an island. They are being

29 October 2013 Nicholas Lansman, Dido Harding and Hamish Macleod

more proactive and generating more intelligence to pass either to our own law enforcement agencies or internationally, to overseas. That will generate more work in other parts of the ecosystem. If we are going to put more resources into the IWF, more resources need to go into other parts of the system too, otherwise we are just creating traffic jams in other bits of the net.

Q88 Mr Sutcliffe: It is good to hear that there is a level of consistency there now. You have talked about the easy work, if you like, the illegal, which is clearly identified as illegal and, therefore, it has to be stopped. One thing that concerns me is the cultural issues that are around. In evidence at the last session, 30% of children under the age of 12 thought it was okay to be bullied or had experience of being bullied on the net. Notwithstanding the massive amount of work that it has done to deal with the illegal situation, how do you deal with the cultural changes and trying to get different responses across because of some of the problems that people are already facing through the surveys that already exist?

Dido Harding: I think step by step would be my rather simplistic answer. The number of things that can happen to a child online are just as many as can happen in the playground, only it is more immediate and they have the whole world at their fingertips. The wonder of the internet, as Stella Creasy set out, is that it has a double-edged sword element to it. That is why I go back to road safety. We have to think about all of the different types of behaviour that happen in the playground.

On bullying, I do not think that the fundamental issue is any different from being in the playground. The adult supervising the playground has a role to play. The children have a role to play, as do their parents, and there is a bigger public awareness challenge on all those dimensions because it is so much less visible than your child being physically bullied in the playground. I don't think you can overstate the importance of people such as yourselves thinking deeply about this. The social and moral framework for the digital world does not exist yet.

I do think there is quite an important role for legislators to play in thinking through where the absolute black and white rules are that we need to put in place. There is a clear role for all of the owners or builders of the playgrounds, whether those are the social networking sites or the internet service providers themselves, to think through, "How do you provide parents, teachers and children with the tools to make that environment safer?" There is a clear role for all the educators to make sure that we are keeping up with that technology, not just for our children but in educating parents and teachers themselves.

I wish I could say that there was a magic bullet. There is not. We are the generation that has to quite calmly and logically think through each of these issues.

Q89 Chair: Without wishing to stray too far into the data communications debate, which would keep us going probably for the rest of the day, can I ask you, first of all, how much data in terms of which individuals are accessing sites, downloading images

and sending abusive messages do you keep and how easy is it for the police, for instance, to have access to it?

Dido Harding: I am very happy to answer for TalkTalk and you can fill in the gaps. Obviously we work under RIPA. From a TalkTalk perspective, we currently provide call data, IP addresses, subscriber details both for our mobile customers and our fixed customers, session details, so how long they have been online, IP log history and data access setup, so how they are accessing it, and we will also provide email addresses, payment details, customer notes and email headers. All that is governed by RIPA. We store those data in the same way that we would store our own customer data. We retain data for 12 months. We respond as quickly as all the Government authorities accessing through RIPA require of us, and are compensated for them for doing that. I think that process works reasonably well. I would be disappointed if you heard otherwise from those authorities.

Chair: Would that cover Twitter postings?

Dido Harding: No. We do not store browsing history; so exactly where you have gone and what you have done, which pages you have looked at, we do not store any of that. That is not governed by RIPA today. I do think it is important that, in this, the ISPs are not choosing their own rules. This is something that is clearly for you, not for my colleagues and me, to make the judgments. We act absolutely within the letter of RIPA and store the data that is required of us there.

Q90 Chair: RIPA itself is now a little ancient in terms of the speed with which things are advancing. Do you think it needs to be revisited?

Dido Harding: I think that the debate that is currently ongoing is very important, precisely as you highlight, Chairman. The tools and techniques are changing so much. Yes, I think it is very important to have that debate and to make sure that we keep up to date.

Chair: Hamish and Nicholas, do you wish to add anything?

Nicholas Lansman: If I can just add to that, as I was explaining, that is a very similar setup to the other internet service providers. I think it is important that, with an extension to the data requirements, the Home Office make their case and pass legislation and that is fully debated. It is very important to note that the ISPs, as they comply with RIPA, will comply with amendments to it if that is the case. Hamish made a point earlier about the fact that we have a lot of data and I think in a previous session Peter Davies, the CEO of CEOP, outlined the fact that there are possibly thousands of potential investigations that perhaps should be taking place if resources would allow. Just collecting more and more data that may well be useful will point out an even greater problem in the lack of resources to follow up.

Hamish Macleod: I do not have anything in particular to add to that.

Chair: Basically your industry follows the same practices that TalkTalk has described?

Hamish Macleod: Yes. There are a few technical differences but it is, policy-wise, exactly the same.

29 October 2013 Nicholas Lansman, Dido Harding and Hamish Macleod

Q91 Chair: It does not matter if I am using a mobile device or a fixed broadband device? The same provisions will apply?

Hamish Macleod: More or less. I am not entirely sure what the fixed situation is. In mobile there is not necessarily a one-to-one mapping between the IP address that is being used and the user because we do not have enough IP addresses to go around. We use something called NAT, network address translation—he says quietly—and that generates an absolutely enormous amount of data.

Q92 Chair: If I used a mobile device in Starbucks, are you able to identify that it is me?

Hamish Macleod: Connecting how?

Chair: On a public wi-fi system.

Hamish Macleod: I don't know I am afraid.

Nicholas Lansman: I am pretty sure that the providers of the public wi-fis, whether it is in Starbucks or anywhere else, are also covered under the legislation. Whether it is BT or other cloud providers, they will be able to provide that data to enforcement. It is worth underlining—

Chair: But it is not much use to know the person who has accessed inappropriate material from Starbucks on Victoria Street.

Nicholas Lansman: I think another discussion that we will possibly have is the issue about anonymity and whether that can mean you can't trace people. That is not the case. As we found in the previous session, people commenting on Twitter and making comments are subject to prosecutions, just like anyone else. It is worth underlining that our systems have been in place for quite some time and work well. We have single points of contact within the Home Office. They can be in contact with internet service providers simply. The system effectively works well.

Q93 Tracey Crouch: Could I just follow up, just to be clear in my mind, Ms Harding, on what you were saying about collecting all the data and keeping it? That is available upon request under the legislation, but if somebody was accessing illegal content, such as child abuse images, does that flag up in your systems and you can then pass that over, or does it have to come from the enforcement agencies before you give that material?

Dido Harding: As it currently works, we respond reactively to requests from CEOP. It is one of the things that we have been discussing with the Internet Watch Foundation as part of moving the IWF activities to being more proactive; so proactively identifying sites and then potentially proactively identifying offenders. This is all fraught with moral hazard and, in doing something like that, I would only want to consider it with the full legal authority and not as an ISP decide for myself that I fancy doing it with my customers.

I feel very strongly the weight of responsibility as an internet service provider in that our customers place their faith in the fact that it is their data, not our data, to choose what to do with and, therefore, we need a clear legal framework on what we store and what we do not store. That is why I say we store the information that we are required to by RIPA and we

store the information that we need in order to serve our customers. We do not keep browsing history of where our customers browse every day of the week—that is their data, not ours—unless or until there was a change in legislation that required us to.

Q94 Tracey Crouch: But you are able to keep internet browsing and other communications data under the Data Retention (EC Directive) Regulations 2009, I believe. You could, if you wanted to, keep that data.

Dido Harding: Technically we could. There are different views from the lawyers on whether our customers would be expecting us to store browsing history. For example, when we launched HomeSafe and when we first trialled HomeSafe, which is, based on where you are browsing in your home, you have set a series of filters that in your home, for example, suicide and self-harm sites can't be seen. That requires us to store for you that you want suicide and self-harm sites blocked. A number of organisations and the ICO themselves were very concerned that that did not mean we were storing the history of where you were browsing. We went through a number of stages to give the ICO confidence that we were not storing unnecessary information that our customers would not necessarily want us to. That is why I say I am very cautious about what data we store, if it is our customers' data as opposed to stuff that we need in order to run the business for them.

Q95 Tracey Crouch: While I completely understand the moral issues that you highlight about people accessing sites that they want to—I can appreciate that around, for example, online pornography—the issue about illegal images of child abuse, for example, is something completely separate.

Dido Harding: Yes, I agree. I do agree.

Tracey Crouch: If you are seeing information or data from your customers, who are accessing sites that are illegal, does that not have a moral duty on you as a provider?

Dido Harding: I completely agree. If you are starting to think through the stages at which it would be appropriate to expect ISPs to pass that information through, the easiest and most obvious is illegal child abuse images, which are illegal to look at, illegal to create, illegal to pass on, and it is a criminal rather than a civil offence. I do agree with you and that is why, through the IWF, we are working through a process to do that. It is much less obvious as you work your way back, because I do not think our customers want internet service providers to store their history of which car sites you have visited so that we can sell it to car manufacturers for you to be bombarded with emails about buying cars. It is very important that the ISPs do not feel like it is a free-for-all to use that data. Our customers do not expect that of us. We have been thinking through, if it is entirely criminal, how we get to a place where we can do that proactively with CEOP.

Q96 Tracey Crouch: In our first oral evidence session, we heard some shocking statistics about child abuse images on the internet, talking about millions

29 October 2013 Nicholas Lansman, Dido Harding and Hamish Macleod

of images. 81% of those images involved children under the age of 10, 4% of children under the age of two, and over half of them were level four or level five images. Do you think that the ISPs are being effective at blocking these sites, these images?

Dido Harding: We are only as effective as collectively through the IWF we are effective at identifying the images. I think we all recognise that the reactive approach, although it has taken the UK to a much better place than a number of other countries, has not solved the problem. Hence all the ISPs are committing to increasing the funding of the IWF so that the IWF can proactively go out and identify sites that we could all block. No, I do not think anyone working in the industry can say, "Yes, this is a job well done". It is a job that we know we have to do a lot more.

Tracey Crouch: Do you have anything to add?

Nicholas Lansman: I think it is fair to say that there is no complacency in this area. While the internet industry is quite proud of having set up the Internet Watch Foundation, it is an ongoing battle and I think that several changes are taking place over time to make the IWF more effective. It is true to say that, of child abuse images, less than 1% are hosted in the UK, but they are still going around the world. The IWF also works with bodies abroad to make sure they are trying to get them blocked at the source, because I think that is the priority. Blocking is part of the solution, but for the internet industry it is more important that we try to remove this content at the source, whether it is in the UK, more likely to be elsewhere, in the US and so forth.

In addition to the extra resource that the IWF will be getting through additional membership payments from members, there is also a development in terms of delivering splash pages. If someone accidentally comes across child abuse images, rather than getting an error message that just stops them accessing the site they will now start to get splash pages that will identify it is illegal material and they should not look at it. These are some of the developments that are taking place, but you are right. There is no complacency and the internet industry continues to work with the IWF, but also with CEOP and under areas of law enforcement to make sure that the battle to get rid of child abuse images and protect children online continues.

Hamish Macleod: The Government has announced that it is joining various international alliances to tackle the problem. At the moment, the impression I get is that it is all still a little bit aspirational and they are just finding their feet. Those alliances need to have clear deliverables and a clear action plan to improve the situation because, for a great number of years now, the vast majority of these sites have been hosted outside the UK and international action and co-operation is what is going to lead to them being removed and the people who are putting them up there prosecuted.

Tracey Crouch: Do you think that requires a will or money, or both?

Hamish Macleod: I am sure it will require both, yes.

Q97 Tracey Crouch: I understand that TalkTalk automatically downloads the blocked list of known websites containing illegal images on a daily basis. Is that right?

Dido Harding: Yes.

Q98 Tracey Crouch: Two related questions. First, do you think that a daily basis is fast enough and what time of day do you do it? In my mind, if you are doing it in the morning, by the time people are accessing in the evening, probably new sites have popped up or been created. It is just out of interest.

Dido Harding: I am ashamed to say I do not know what time of day. I will check for you.

Tracey Crouch: I would be interested to know, because it is such a fast-moving beast. Maybe I have some sort of prejudice that these things are only being accessed in the evening, but I just wonder—

Dido Harding: You are quite right. Let me go back. I will get that for you. I can't speak for the other ISPs. For TalkTalk, it is currently a manual process. There is a temptation to believe that telecoms companies are all entirely automated. I wish we were. My goal is to be able to automate it. Then I should be able to consume it much faster.

Nicholas Lansman: I will check, but I understand that twice a day there is an update to the list.

Chair: That is updated twice a day?

Nicholas Lansman: Yes.

Dido Harding: Then we consume it once a day.

Chair: You only do it once a day.

Q99 Steve Rotheram: I think Tracey has elicited a response for the first question I had, so if we move on. Is there a case for more effective filtering of legal adult content, which could be obscene if it was viewed by a child?

Hamish Macleod: The mobile filtering has been in place since 2005 and it covers what we describe as age-inappropriate. The framework that decides if it is age-inappropriate or not is given to us by the BBFC and it covers violence, pornography-type stuff, behavioural stuff such as promotion of suicide, promotion of anorexia, those sorts of sites; all the topics that are of major public policy concern are covered by their framework, whether that is obscene or just 18-type content that you would see in the cinema.

Q100 Steve Rotheram: Information is filtered. There are filters. How effective are the filters?

Hamish Macleod: I believe they are very effective. The accusations that are thrown at us more often are about over-blocking of content, where we get a handful of reports each month about accidentally over-blocking. Again, part of the reason for the move to the BBFC is to make that process a little bit more slick so that if a website owner or a member of the public believes that a site is being over-blocked, or under-blocked, they are able to report it and the first port of call is for their mobile operator to look at that. Most of the time it is accidental and it is fairly easy to speak to the filtering company and say, "Please can you just change the categorisation of that website so

29 October 2013 Nicholas Lansman, Dido Harding and Hamish Macleod

that it either is not blocked or is blocked, as appropriate?"

Q101 Steve Rotheram: They are filtered at network level?

Hamish Macleod: Yes, that is right.

Steve Rotheram: How about at mobile device level?

Hamish Macleod: Not very often, no. The products that are available in the market to filter it at device level tend to be a bit blunt. It is either about "turn on the internet" or "turn off the internet", or they whitelist a very few sites or blacklist a very few sites. From our point of view, it is an area that we would like to see discussed a little more in the public domain because a lot of the focus has been on what can be done at network level, but what can be done at browser level, what can be done at operating system level, what can be done at the content provider level or what can be done at device level? They all have a contribution to make to this so that people can tailor the services and the protections they want as best they can, but we do the filtering at network level in accordance with the framework that is independently provided for us.

Dido Harding: I would say that there is still an awful lot to do to improve the quality of filtering tools that you give parents. We have had HomeSafe in the market for 2.5 years. I would be the first to say that it is not perfect and that there is a lot more to do to make it something that is easier for parents to understand and give some of the tools. Firstly, I think it is important to remember that parents are not just interested in blocking adult content. They are, if anything, more worried about suicide and self-harm. They want to block gaming or gambling. At certain times of the day they want to block access to social networking so that their children do their homework. It is important to look at this more broadly than simply the, admittedly, very serious issue of the wealth of adult content online.

First, thinking about different types of content. Then also we think whole-home network-based solutions play a very important role, but they are not the only solution. If you have teenagers and very young children in the same household with multiple different devices, you will want a more sophisticated filtering solution that enables your 16-year-old to do their homework, while it absolutely ensures that your three-year-old cannot stumble on something that they are not expecting. The parents themselves may want access to some of those different sites.

We get customers complaining that they have turned on HomeSafe and all the filters, one of which is for alcohol-related sites, and that blocks Waitrose wines. We know that the technology is not quite there yet. When my competitor ISPs launch their network blocking solutions, I am expecting that they will be better than mine in some ways and that will be a good thing. This is still an area where innovation can get you a march against your competitors and there is real consumer demand for tools that are simple to use but meet their needs. I would want the Committee to feel that both mobile and fixed-line telcos recognise this is something that we have to keep working at, because

our consumers tell us loud and clear that we do not quite have it right yet.

Nicholas Lansman: Just a couple of issues. I have previously mentioned over-blocking and under-blocking, which is taken very seriously, but I think it is important to note that, while the technology is improving and will continue to improve to make sure that parents have a tool that they can use in their homes to make sure it is age-specific and to ensure their children see only content that is appropriate for them, technology is not a replacement for good parenting.

I know the industry is working with Government and charities to ensure that parents have adequate information and that they can feel confident about how the internet works and also confident in using the technologies, but also to have that dialogue with their children, which is very important. These are some of the points that came out of various Government reviews such as the Byron Review and indeed the Bailey Review more recently, where it talked about a partnership approach to child safety. Industry has an element of responsibility to provide those tools, but equally there is the responsibility for parents and the responsibility for Government also to help with that education process.

Dido talked about how we have had many decades of education to deal with how you drive, use seatbelts, drive safely and do not drink and drive. Equally, there have been campaigns for years about learning to swim, children playing safely with matches, how to climb ladders safely and even recently how to barbecue your sausages. I think it is important to note that this education, which some of your questions earlier referred to, is how you get this change in how we understand the technology and use it safely. The answer is it will take time and industry is certainly stepping up to the mark and providing those tools and some of the education. We feel it is also incumbent on parents, teachers and the Government to also assist with that education role.

Dido Harding: What we have learnt is that parents value being prompted to think about this. Since we adopted active choice, if you go on to your account page with TalkTalk and you have not turned HomeSafe on, it will pop up and prompt you to say you haven't and, if you have children in your house at any time, we strongly recommend you do. We find that the vast majority of our customers welcome that interruption and the vast majority of them with children at home turn it on as a result. I do think this is a space where proactive action from all the participants is required. It is not just going to happen by osmosis.

Q102 Steve Rotheram: But any parent of a certain age will know that if you have a technological problem then the first person you go to is the 12-year-old or 13-year-old. How easily can children circumvent these filters?

Dido Harding: Nothing in life is perfect. We lock the doors of our houses, even though we know a burglar could get in. I would not want to pretend that our safeguards are 100% perfect, but if you change the HomeSafe settings the account holder gets an email

29 October 2013 Nicholas Lansman, Dido Harding and Hamish Macleod

immediately saying that you have done this. The only way, in our system, that your 12-year-old could get control of the filtering is if your 12-year-old is also paying the bill for your home phone and broadband. In order to do that they will have to set up a direct debit, which they will not be able to do at age 12. Clearly, some very clever 12-year-olds may well have masqueraded as 25-year-olds and be paying the home phone bill, but all our analysis suggests that is very tiny percentage. That closed loop where the accountholder is automatically informed if any of the settings are changed and you can only set them if you are in the account space where you pay your bill is our closed loop.

Hamish Macleod: In mobile, you would go through an age verification process before you can take the filters off. On the education point, this something we have been again plugging away at for years and years and years, both individual operators and collectively; distributing materials within the schools to support teachers. It is not just about inappropriate content, of course. It is about inappropriate behaviour. It is about making sure you have physical security of your device—do you have a PIN number on your mobile to prevent unauthorised use, to prevent from people going on to it and spoofing you—and protecting your personal data and all that sort of thing.

For years we have been putting this stuff into the schools. I am not fully convinced that the Government is giving it enough support within the school system, because that is the easiest point to access children in a formal setting. It should not just be about the ICT doing it. It is about all teachers. Through the teacher training programme, teaching them how to use technology in the teaching environment, but also how to use it responsibly and safely and encouraging children to behave responsibly because it is their behaviour that is so critical.

Q103 Mr Leech: Can I just ask why TalkTalk decided to become the first ISP to have this unavoidable choice?

Dido Harding: We decided to build HomeSafe about five years ago before I became the chief executive. It was my chairman and my chief technology officer's brainwave that we could build a whole-home network-based solution. We have a much younger, simpler telecoms network—techno-babble for a second, an all-IP network—that makes it technically simpler and easier for us to do it and our customers told us that they were really worried about it.

Unashamedly, we launched HomeSafe because we thought it was brilliant for us as a business, that it made good business sense to offer our customers something they wanted, and to bundle it in for free with our product. I can't take any of the credit for that. It was my chairman, before I even joined. We stand by it. It cost us of the order of £25 million to build and a lot of people thought it was not possible to do. There are not many things, to be honest, where in TalkTalk I am saying I have done something that my competitors are about to do. We think it stood us in very good stead, that our customers who use it are much more loyal to TalkTalk as a result. It has been a good investment.

Q104 Mr Leech: What stopped other providers from doing it before now?

Dido Harding: I am probably not the right person to answer that question.

Nicholas Lansman: I do not want to speak on behalf of the other three main providers.

Mr Leech: You can have a guess.

Nicholas Lansman: The point is now that this code of practice has been agreed by four of the main consumer-focused ISPs. They all agree that active choice or this unavoidable choice—so when you have a new customer, they ring up or contact you on the internet, they have to make that decision about whether they want to turn on parental controls—is now agreed across the board. It is good that TalkTalk were the pioneers, in that sense, but I know the other players in the industry are stepping up to the mark. We have introduced a whole range of child protection measures. We have talked about choice. We have all talked about the filtering for free, right across the board, through the whole home. These are just some of the developments that have been taking place over the last year and will continue into 2014. There has been a huge investment and some major developments of which the whole industry is quite proud.

Dido Harding: I would say, on a broader topic, what you have in the UK telecoms market, both fixed line and mobile, is two very highly competitive markets. The BBC ran something yesterday on, "Why is it that in the US you have to pay so much more for your broadband?" and the basic answer is because there is no competition. What you have in the UK, in both fixed and mobile, is two very competitive markets. Fundamentally, we did this in TalkTalk because it was something that we were willing to take a risk on that our much bigger, maybe slightly more bureaucratic—you never know—competitors were focused on other things. As you as a Committee are looking at this industry as a whole, recognising the power of competition to make sure that you have technological innovation is important in this sector.

Q105 Mr Leech: You said it cost you £25 million and, from what you said, I guess that it would have cost more if you did not have such a simple system.

Dido Harding: Yes.

Mr Leech: So, is it cost that has put off the other providers before now?

Nicholas Lansman: I do not think it is. I do not know what the costs have been for the other systems put in place by the other main consumer ISPs, but it is a very competitive market. All ISPs will have different priorities in terms of where they are in the marketplace. Obviously providing good, fast broadband is an absolute priority to all the companies and providing it at a price that people can afford. There are still 7 million people that are not yet connected to the internet in the UK; not all of those have children. There is a range of issues that companies focus on to deliver fast broadband at a price that is affordable for the UK market.

Q106 Mr Leech: One of the issues of debate at the moment is whether the active choice should be about whether you opt in to adult content or opt in to filters.

29 October 2013 Nicholas Lansman, Dido Harding and Hamish Macleod

From TalkTalk's perspective, do you have a difference in take-up of filters from people who buy broadband face to face or buy broadband over the telephone, as opposed to over the internet where it is all far more anonymous and people perhaps are less embarrassed to take a particular view on whether they should have filters?

Dido Harding: 99% of our customers are buying over the telephone or online, rather than physically face to face. We do not see any difference in the take-up of HomeSafe based on whether it is an online sale or a telephone sale. As a general rule, in all things we sell, we see much higher customer satisfaction when they buy it online, when they are in control of their own settings and it is easier for customers to configure online than it is to have an agent. As we have just been grappling with in the last hour, the technology is quite complicated. Describing it to somebody who is not hugely digitally savvy over the telephone is not easy. I always worry that people buying the product over the phone might not understand what filters they have turned on as clearly as someone buying it online.

Q107 Mr Leech: Do you find, once people have opted in for filters or not opted in for filters, they often change their mind and change it at a later stage?

Dido Harding: Yes. They turn them on and they turn them off again. I remember keenly when my husband was at DCMS himself discovering that the *Racing Post* was default blocked in our house because I had blocked all of their HomeSafe categories and, as racing was one of his areas, he was a bit cross. Immediately you will want to change that.

Mr Leech: It is one of your areas as well, though, isn't it?

Dido Harding: Yes. You see, that is what our customers tell us. They do want to be able to change the filters because their children change, their lives change and, to keep the tools simple enough—it is still quite blunt. As I say, you blocked alcohol because you do not want your 12-year-olds going on to alcohol abuse sites but then discover that wine retailers are blocked, so you want to change that.

Q108 Mr Leech: You have recognised that the filters are getting better?

Dido Harding: Yes.

Mr Leech: Have you seen a decrease in the number of complaints or queries about a site being blocked or not being blocked, in the time that you have been offering the service?

Dido Harding: As the base has grown and our customers are getting better at understanding it, we are seeing an increasing desire for us to make the product better. Our customers would love us to have the ability for them to white-list a particular site within a category. For example, the national lottery would count as a gaming site. There are an awful lot of families who are buying a lottery ticket each week. They want to check the winning numbers, but they want gaming sites and gambling sites to be blocked. At the moment, our HomeSafe tool does not enable you to do that. We have seen an increase and I think it is a good thing that our customers are engaging in the product, because the thing you do not want is that

they set the filters and think that the internet is safe now for their family and they do not need to worry about it.

Q109 Mr Leech: How far are you away from being able to white-list individual sites?

Dido Harding: Not very far.

Mr Leech: How far is not very far? Six months, six years, 60 years?

Dido Harding: With some of my competitors in the room, I would rather not give you a specific timing, but we are a pretty entrepreneurial business that tries to do things quite fast.

Mr Leech: I am guessing it is quite technologically difficult, then?

Dido Harding: No. I am not an engineer, so I bat away all the hard work, which is very unkind of me, but a lot of this is more around the amount of changes you can make at any one time to a stack of code. It is not that it is technically difficult to block a specific site and give a customer permission. It is just hard to get all the work done that everyone would like to do in it.

Q110 Mr Leech: Turning to social media, how easy is it to trace people who set up fake identities on social media sites?

Nicholas Lansman: I know you are taking evidence from some of the social media companies later, so I do not want to go too much into this area. I mentioned before that I think there is a difference between anonymity online and that does not mean you cannot trace people. In the previous session with Stella Creasy we had good examples of where people try to hide their identity online, yet they have been in the process of prosecution. People can attempt to hide themselves online, but there are technical ways in which they can be discovered. We talked about IP addresses and so forth.

Mr Leech: Is it straightforward, though, technologically?

Nicholas Lansman: I do not think it is straightforward. I am not technologically competent enough to give you a direct answer to that, but we can go away and perhaps provide some further evidence to the Committee on this point. A lot of this is possible, but some of the issues that were considered by Stella Creasy about people creating multiple fake identities is an issue the social media companies are looking at, at the moment.

Q111 Mr Leech: Do any of you have a view on whether social media companies could do more to combat illegal behaviour?

Dido Harding: I would take the view that all of us participating in this space can do more. I would not pretend to know enough about what social companies could do specifically, but I think you should be pushing us all.

Mr Leech: What, in your view, is the reason why they are not doing more at the moment? Is it because of this view about freedom of the internet or is it about money?

Dido Harding: I thought that, in the earlier session, Stella Creasy was right. She was talking specifically

29 October 2013 Nicholas Lansman, Dido Harding and Hamish Macleod

about Twitter. These social media companies are just very young and they have grown exponentially fast and they are catching up with some of these issues. I do not think you should just label it, "Is it money or is it technical ability?" A chunk of it is immaturity of an industry, that we are all learning how to do this. That is why you should be holding us all to account to think it through.

Q112 Mr Leech: When you say, "Immaturity of an industry" though, is it something to do with the uniqueness of social media companies that seem to be able to grow exponentially with a very small number of staff and just literally do not have the capacity to do the work that needs to be done without a vast—

Dido Harding: If you take my road safety analogy, it is the sheer speed at which these organisations have gone from being a garage business with a group of people in their early 20s to being a Fortune 100 company. The speed of that growth does put pressure on any organisation to catch up, in a world where the moral and social framework does not exist yet.

Nicholas Lansman: Added to that also is that many of these social network companies are global and the

Committee is also looking at this concept of how companies can know how to comply—well, they need to—with the law and to interpret it. It is not so much that the companies are not willing. It is a complex situation where, even where laws apply online as well as offline, it is how to get to grips with them and how they can work with law enforcement as well. As Stella Creasy said previously, it is an evolving area and I think technology companies, whether social network or otherwise, are part of this learning process.

Hamish Macleod: The volume is high. A number of years ago, I appeared in front of this Committee and I remember quoting a statistic that something like 10 hours of YouTube video goes up every minute. I heard that statistic the other day and I believe it is now 10 times that going up every minute. It is an enormous volume that is being dealt with.

Dido Harding: In all the work that I do with the social media companies, I see no lack of willingness to tackle these issues. It is a scale and scope challenge for all of us.

Chair: I think that is all we have. Thank you very much.

Examination of Witness

Witness: **Mr Jim Gamble**, Independent Chair, City and Hackney Safeguarding Children Board, gave evidence.

Q113 Chair: For our third sessions, I welcome back before the Committee Jim Gamble, who is now Independent Chairman of the City and Hackney Safeguarding Children Board, but whom we also remember as the first chief executive of CEOP. You will have heard some of the evidence that we have taken, both this morning and in our previous session. Can you give us your view of the current degree of the problem both of the extreme child sex abuse-type images and also on the problem of children having access to inappropriate material that is more appropriate for adults?

Jim Gamble: I will deal with the inappropriate material first because it is the easy one. I think inappropriate material is a parental decision for those individuals who have duty of care of the young people to make and I think active choice is absolutely right. If parents and others are prompted to make a decision, I do not think you can do more than that. You are not going to go out into their homes and look after their children for them. We are not going ensure that they do not drink more alcohol than they should or whatever else. I think active choice means that you are prompting a decision that a parent must take.

Apart from that, the reason that it is inappropriate and not illegal is because it is not against the law and thereby it is quite appropriate for the parent or carer or person with the duty of care to make that decision. There is far too great a focus and emphasis on that side of the debate at the minute and it is clouding other issues. If you look at Miley Cyrus or if you look at some of the other pop stars and their behaviour, that has a far greater and much more easily accessibly influence on young people today than seeking out adult or hard-core pornography for that matter. There

is no debate or discussion of any value on that because you have young pop stars who young people want to emulate behaving in a highly sexualised way, whereby there is no filter. That is that issue.

On the second one, I think we have stood still for a number of years because of inertia in Government. Let me say before I start that I am going to speak on the basis of the Laming principles, following his review after Baby P, and that is that we must have lots of professional curiosity and appropriate and respectful challenge. Anything I say is not to offend anyone. It is simply to bear in mind those principles. You have too many images still on the internet. We have too few people deterred from going on and looking at those images. We have diverted the debate from how we stop people from accessing, abusing and capturing images of our children to how we manage an internet industry that has not stood still; who have blocked images for as long as I have been involved in this, from 2002, 2001; who have put in place processes, perfect or imperfect, to deal with those. What we need to do now is address the issue that we are not being creative or imaginative enough in how we turn the tables. Let me give you an example of that.

Peter Davies, in one of his statements to the media, talked about 50,000 to 60,000 people downloading indecent abuse images at any given time. What we know about the propensity of those individuals to go on and commit hands-on offences is sufficient that, if you are a parent, you should be extremely concerned. Ultimately, though, we are not having the debate about how we resource child protection teams and how we identify, locate and rescue the children trapped in these images. I have read the previous

29 October 2013 Mr Jim Gamble

evidence. I do not accept, and I have rung around, that very few of the images are new. Too many of the images are new. The images that you talk about that IWF will access are not hidden on peer-to-peer. That is where paedophiles nest to share their images. How do we identify, locate and rescue those children and how do we identify, locate and hold to account those predators that represent a threat?

You talked about education earlier. Unless you have a deterrent—in other words, we arrest 2,500 people and prosecute them for this—you have no deterrent to point to that is credible in the classroom. Young people understand that. There is a case in America at the minute where two girls have been arrested for bullying. It will be an interesting case to look at later. But let us accept that we have a problem with finance. What I would propose is the Government would be better investing £1.4 million in recruiting 12 detective sergeants, 12 trainers and co-ordinators and using the enthusiasm that is on the ground, because we have seen organisations like Let's Go Hunting. Is that a good thing for them to do? No. Does it represent the manifestation of the frustration that we talk about one issue while our children continue to be abused? Yes, it does.

Let us for one second be a little bit imaginative and take the special constables' role. Why can we not have special constables online? The figures I have given you are ready-reckoner figures, so they take account of not just the salary but also the on-costs of the equipment. If you had that for each region, every police force could recruit up to 10 special constables, just in theory, in their area that would be trained, vetted and supported to come in and give of their time. As a retired police officer, I might say, "Well I'll actually go into Belfast to the PSNI, and I will give X amount of nights a week", the same way as specials do anywhere. If I had worked in IT or currently do that, I might want to give up time.

If you did that, you would have 520 people online at any given time who could manifestly cover 10, 20, 30 or 40 chat-room environments, where you would have people out there protecting our children. Not rogue vigilantes, but properly vetted, properly trained and accredited and properly supervised officers online. To me, that is what we should be thinking about so we attack the root cause, which is people. Not get involved in what I see in the one instance as trying to cover up the fact that—and I have read your evidence, that everything is fine in CEOP. Well, I would suggest you scratch the surface on that if you think that CEOP has not been diminished by going into the National Crime Agency.

To move the argument to, "How can you deal with this problem?" We have all become seduced by the technology. So we talk about filters and we talk about blocking. We have been doing that for a long time. I sat and listened to friends from the internet industry. They have been doing a good job for a long time. I have not always been their greatest fan because they should be pushed and they should be challenged, but I have not heard any talk about the Click CEOP button that children can go to in Facebook if their parents have downloaded it, and report, and we fought long and hard to get that put in there.

In 2004, when I was deputy director general of the National Crime Squad, we created a site that was bogus. When you came to it looking for child abuse images, it popped up and said, "This is a law enforcement site. Your IP address is—. You have committed a criminal offence." Those issues were okay in their day, but it seems to me we have stood still. Matt Bishop, vice president from Microsoft who sat on my board in CEOP, said, "The thing you must remember", and I would challenge you to remember as you go through this, "is that in the world of technology, standing still is falling rapidly behind".

I believe we have fallen behind. I believe the early success of CEOP—not because of me but because of people like Helen Penn and the education team, who is now working for some other unit in SOCO, not dealing with children, a fabulous child protection expert, developed all the early CEOP training and education materials, had worked for Childnet charity, but is now working in some other part of an organised crime entity. It does not make sense. We need to reflect that this is about people. The internet industry can be attacked for so long, but we have to get to the point where we say, "How can law enforcement do more?"

Chair: Thank you. We are going to come on to the CEOP incorporation issue but before we do, I will bring in Steve Rotheram.

Q114 Steve Rotheram: Before we do that, I followed the line of questioning last week about the victims in this. It is surprising that Jim has come up with a very different explanation of that from Peter last week, which is very concerning because one of the priorities for me was what we do about trying to prevent other people from becoming victims and what we do to help those people who are the victims. How far do we pursue that? Perhaps my line of questioning did not go far enough, but you are saying that we do not do enough in that respect?

Jim Gamble: We do not do anywhere near enough. CEOP now have—I will estimate—two people working on victim identification. Police forces are dealing with 101 other issues out there. How many of them do you think have dedicated resources right now looking at these issues? I have read the statistics, the 26 million. That is five forces. You are looking at millions upon millions.

In one investigation we did, Operation Cathedral, there were 750,000 images, but they related to 1,232 or 1,233 individual children. On peer-to-peer, these are being created. On the 50,000 Peter talks about, those are peer-to-peer sites. Those are hard-core paedophiles who do not stumble across anything on Google. They nest in these places on the internet where they can share secretly. You have to infiltrate that. You have to infiltrate it. You have to identify who they are and follow them offline and arrest them.

During Operation Ore there was massive controversy, but you know what? In the UK, we identified, located and arrested more than anyone did anywhere else in the world. I am now more convinced than ever that what we did was right because, for a short period, people were afraid to go online and download these images because they could be arrested and exposed to

29 October 2013 Mr Jim Gamble

the full glare of daylight, and they do not like that. You do not have an active deterrent. If you look at the last two years' CEOP reports, the arrests are lower than they were for any year except our first year of operation. That cannot be right. That is not a deterrent.

Q115 Chair: Just on that point, we came to visit CEOP when you were running it and you ran a programme over 24 hours, peer-to-peer file sharing, and I think you came up with something like 20,000 sites making available hard-core images. Those are 20,000 IP addresses that you could identify and you could go and raid them or arrest them, if you chose to do so. Is it simply a lack of commitment or resources that is preventing that?

Jim Gamble: It is not lack of commitment anywhere. Peter Davies and everyone in CEOP are absolutely committed to doing the right work, as are people in all the police forces around the country. I think we become seduced by all this and, because of the volume, we say we can't do anything. To use the CEO of TalkTalk's example, if we did not enforce speed limits on the roads we would have hundreds of thousands of people committing those offences, but when they see a picture of a speed camera on the side of the road they slow down because they realise that the deterrent is real and they may in fact collect points and lose their licence. We need to get to a position where we stop dealing with some of the technological issues that have seduced us for so long and attack the issues, which are people.

To come back to your point about victims, we need to get into the images to identify those children who are new victims, those children based in a particular geography, so we can share that with law enforcement abroad or do more. Two people working all the hours that God sends are not going to make that difference. I am recognising the financial restrictions and everything these days hides behind austerity, but for about £1.4 million, giving the public, retired officers and others the opportunity to engage you could make a huge step-change and difference. That is about being child focused and not being organisationally or politically focused, in my opinion.

Q116 Steve Rotheram: Moving on to the other aspects of it, we know that possession and publication of child sex images is illegal. Are there any changes in legislation that you think could help the police do their job better?

Jim Gamble: You can always tweak legislation. I heard your earlier comments on that and I would not disagree that you might want to refresh the language. My issue is that we do not need new legislation. We need new thinking and we need people to apply the law as it currently exists.

When I listened to the Member of Parliament giving evidence earlier, Stella Creasy, I was struck by how well she encapsulated it all. The Prevention of Harassment Act is bullying. The Prevention of Harassment Act is trolling. But we do not have examples that we can take into the classrooms and say to kids, "Don't bully a friend to death. Don't join in this bullying because of these two 15 and 16-year-olds who have been prosecuted." When I say that at public

events and venues people, especially from the third sector, will say to me, "That's not right. You cannot criminalise children."

If a 15-year-old walked up to the bus stop and punched you in the face, we would not say, "Well, you're only 15 or you're only 16. That's okay." There would be consequences. The internet is just like a public place. We need to ensure that the laws as they exist, when they can be applied, are applied. In my experience you can track back. The thing is the child who uses their phone or their laptop or if they are old enough to have one of those old stationary computers that three people would lift onto a desk in a bedroom, they are leaving an evidence trail that is ultimate very, very easy, to follow once you pull the first strand. Educating children in the classroom is key. Where you have two people at the minute—two people, I am told—in CEOP who are currently qualified to deliver the ambassador training, because focus is now criminal justice and NCA rather than education and social care, how do you get into the classroom? None of the resources that are going out at the minute include workshops on Snapchat, on Vimeo, on Vine, on Ask.fm.

While you might have two or three lines on the internet, getting into the classroom where you engage in a virtual cycle: the teacher, the child, and critically, their parent. Parents will complain and bang the table for the three days after something terrible has happened and then they go back to their normal lives because they do not want to think of it happening to their children. The psychology of it is you think, "Well, that is terrible". That is why I think we have had all of this from those poor children that were murdered by Stuart Hazell and—I am trying to remember the other guy's name, but after Tia Sharp and April Jones' murders.

What we have is this reaction, this overwhelming urge, because we are all so emotionally engaged with our children, to demand that something is done; but rather than demand that the right thing is done and we deal with people, we begin to deal with technology. That is a huge problem about focus. We have to look at how we get to the root cause, identify, locate and hold to account as many of those people as you can, which will deter the vast majority from coming online. They do not want to be caught. They can walk into a police station if they want to be caught. The only time you ever hear a paedophile saying, "This was a cry for help", is after they have been caught.

We need to see more being arrested and you are not going to do that with splash screens. If you are a hard-core paedophile and you search for an image and a splash screen says, "You can get in trouble", I do not know—do you think these people grew up in a society where they did not realise the stigma involved? Do you think they kept the secret about the way they engaged and abused children all those years because they thought it would be somehow acceptable, that they need a prompt to remind them that it isn't? That just does not make sense and it is a diversion of attention and resource that does not work. We tried it.

Q117 Steve Rotheram: Again, I am for splash screens, but not for the reason that you are say; not

29 October 2013 Mr Jim Gamble

for the hard-core paedophiles out there. They are far more sophisticated than that anyway. That would not make a blind bit of difference, but as a warning to others perhaps and to try to change the culture online, because I think that is very different to what happens offline.

We all know these sorts of images are illegal throughout the world. For me, I wonder why there is such a prevalence of them if everyone knows they are illegal. Is there a lack of resource from the police to try to tackle it or, as I asked Peter last week, is there a problem with international co-operation so that we need to clamp down on those people who are the main purveyors of these sorts of images?

Jim Gamble: In 2003–2004 we created the Virtual Global Taskforce, which is an alliance across international territory: the Royal Canadian Mounted Police, the Australian Federal Police, Department of Homeland Security, Interpol and others. I was its first chair. In one operation, over 357 hours, I think it was 132 children that we rescued. You need to be online. You need to be patrolling 24/7. I come back to imaginative cost-effective solutions. If a police officer in the UK is working an 8-hour shift, they hand the baton to an officer in Canada, who hands the baton to an officer in Australia, you have 24-hour coverage for an 8-hour shift. We need to go back to those basics, because it seems to me we have stood still. The deterrent that existed during Operation Ore, the deterrent that existed during Operation Chandler—to put the splash screens in context, I would not be against them if the splash screen was saying, “122 people have been arrested this year. Do you want to be 123?” While I was in CEOP, we took an ad out at Christmas in *The Times* saying, “Go online and search for indecent images of children and we will present you with a criminal record”. I am not against that per se, but it becomes laughable if you do not have the publically visible deterrents of people being held to account in court.

Q118 Steve Rotheram: Is the real problem that if there were 50,000 people who were accessing these images, which are all illegal, and those people could be charged and, if they go through the judicial process, could be fined or imprisoned—hopefully imprisoned—that we just do not have the infrastructure anyway?

Jim Gamble: Here is the question. Can they all be identified, located and held to account? How do you know that Bridger was not online looking for those? The issue for me is always this. In my role in safeguarding now, in the work that I do as a consultant and elsewhere, you see people popping up all the time as teachers or in other roles who were downloading these images six or seven years ago. The courts have to take it more seriously. You have a situation now where you will still see teachers, for example, getting prosecuted for this and not going to prison.

At one stage, before my clash with the Home Secretary, in an interview I did say that I recognise that there was a role for cautions and managing some people, but that is about the risk assessment of them. There was a hue and cry that I should have resigned then and many years earlier. I recognise that there is

a role to be played around that management, but the more I have watched the situation develop the more I believe we need to see substantial numbers of people held to account. Courts need to apply meaningful sentences. Courts need to avoid making statements that diminish or trivialise the issue because it is an image.

They need to be asking questions about whether these images have been interrogated, whether we have exhausted every opportunity in the images you have to identify and locate the child, because I will bet if you go out to the police forces who have millions of images they have not all been viewed. If that was one of your children, would you be more interested in that being viewed so that they could be rescued from the abuse that they are probably not telling you about or would you rather that we had a splash screen? For me it has to be children first. That is why this debate is so important, because we have become seduced by statistics and technology and they become images. I have heard people like Claire Perry talk about the fact that these are all crime scenes. Well, yes, great. We coined that phrase in 2004–2005, but the fact of the matter is we are still having the same conversation. It is getting into that. Let us find the kids. If you find the kids, you will find the people who did it. If you hold those people to account, they will not be doing it any more. We have seen in the Savile case that there is never just one victim. There are always multiple victims with these people. If you are able to do that, you are going to create a more active deterrence because the only way to manage paedophiles is through fear, in my experience: fear of capture, fear of exposure.

Q119 Mr Sutcliffe: At the risk of trying to reopen old wounds, Jim, I asked Peter Davies last week if it was a good thing that CEOP had been incorporated into the National crime Agency. He said he thought it was absolutely a good thing. His argument was that CEOP had evolved and that the National Crime Agency brought in wider resources. Clearly, I do not think you see that as the case. Given the solution in terms of how you see a potential solution in terms of where we are, what are your concerns and worries and do you still have those worries now about what has happened to CEOP?

Jim Gamble: I came in from Victoria this morning. I took a taxi across to the hotel where I am staying and we drove past CEOP. As we drove past, there is a big wall where the CEOP sign used to be and we used to have all the photographs of kids who came in from schools. There is now a big sign on the wall that says “National Crime Agency”. The Home Secretary, of course, said that the Government would invest in CEOP and build on its success and that it would not dilute or diminish its operational independence or brand. I have done a lot of work in the last couple of years as a consultant around brand, around social media and everything else. Putting up a National Crime Agency sign is not about not diluting the brand. That is about the bigger brand suppressing the smaller brand because it needs now to establish itself, which is a good example of why it is not right. Child protection in every other sphere has to fight its corner.

29 October 2013 Mr Jim Gamble

The idea in CEOP under *The Way Forward* paper presented by the previous Government was to build on its early success as a consolidated centre, not around criminal justice, but around child protection. I do not disagree that CEOP could have been consolidated somewhere else, but it would have been much better consolidated as an agency of the Department for Education than in the National Crime Agency. If you want to consolidate like-for-like resources, then put counterterrorism in there because, as a former Head of Counterterrorism in Belfast and Deputy Director General of the National Crime Squad, I do know a little bit about organised crime and terrorism. There are many things that are familiar.

To take a child protection agency and put it into a national crime agency where the brand has now been diluted, where they will continue to have protection under Freedom of Information, which is fundamentally wrong, how can you have a child protection entity that is not subject to Freedom of Information? You have a child protection entity that is answerable through the NCA to one political person, the Home Secretary. Where is the credible reassurance around that? Where are the lessons of serious case review around professional independence and challenge? The fact of the matter is we had planned the three pillars to be education, social care, and criminal justice. We now have moved to one pillar, which is criminal justice.

I read the evidence of last week with real interest to see where the statistics are—let us drill into them and see where it is—and I could not see any because it was, “We are not sure about this number, we are not sure about that number, but this is improving and that is much better”. Where is the evidence? Two people qualified to deliver ambassador training in the UK. I do not know how many hundred thousand teachers there are in the UK, but it is a lot.

I do know, from feedback I get at the conferences where I speak and the other work that I do, that there is a frustration that they are no longer able to get the resources. Two fantastic people trying to do a difficult role, but with no resource and no support. Why are there no Ask.fm workshops coming out of what they do? Why are there no Snapchat lessons for the classroom? Why is there not a programme of work that joins up with schools, children and parents together so that you capture the digital footprint of the family and you understand how you then engage, so that the child learns to block, report, do privacy settings with the parent?

Those were all the plans, the 24/7 command and control centre that should have been in CEOP manned by child protection professionals where you could phone in if you had a child trafficking, child exploitation or child abduction issue. Where is that? Gone, subsumed into something else. CEOP's brand was important because it delivered reassurance and it had a high profile brand. Do you think that brand is still as high profile today? The places that I am going to and the people I am speaking to are saying that it is not. I was at the Police and Crime Commissioners Conference in West Midlands, several hundred people dealing with child protection, not three weeks ago. Bob Jones was there. I asked, “Do you think it would

be easier for a child to approach the NCA or CEOP as old?” Of course, maybe they just want to make me happy and I accept that, but I do not think everybody is that keen on making me happy; not a single person in the audience, and there were some from the Serious Organised Crime Agency as it was then.

I will give you one other example. CEOP's academy, partnership with Lancashire University, looking at the psychology of offending, because we need to understand why these people do what they do, so we can interdict it earlier. Where is it? It has gone. It is not happening. For the last three years it has been suspended. Why? Why do we not have that learning being distilled from those interviews and shared with all of the police forces that are engaging and interviewing these people on the ground? It is about having a child protection focus and not having an organisational one that is about facing drugs, facing all other forms of organised crime.

One of the reasons I resigned was because 32 organisations made submissions about CEOP going into the National Crime Agency. None of them, as far as I am aware, supported it from the Association of Directors for Children's Services through the NSPCC and everybody else. Today, with the gift of hindsight, they may say, “Well, it is not too bad”. Do you know why? The Government of the day is the Government of the day and nobody likes to fight with them, but why have those reports never been released? We tried to get them several years ago and under Freedom of Information they could not be released. It is not plutonium poisoning. This is about child protection and what experts' opinions were at the time.

I think we suffered because of a bloody-minded approach of the present Home Secretary at a time when Government was new. They did not, as everyone in child protection knows, do that critical thing, which is pause, reflect and plan before you change anything around child protection. I think what we have seen is an increase in the number of images available, an increase in confidence of offenders and a decrease in deterrence.

Q120 Mr Sutcliffe: I am grateful for that and, not surprisingly, would support all that you have said. The issue for me when I was Probation Minister was the multi-agency approach of dealing with offenders who came out and had to be monitored under licence or whatever. We seem to have lost that link in terms of online safety with those perpetrators, who usually have multiple convictions, who come back out into society and have to be monitored by the different agencies. Has that work diminished or is it still there in terms of the relationships with the other parts of the criminal justice system?

Jim Gamble: I do not know. All I can say is the plan was, in the 24/7 command centre that was envisaged under *The Way Forward*, that there would be, for those critical high-risk offenders, a means for lifetime monitoring them. We were looking at a number of providers around that, so that you would have a centre. Whether a family was in Portugal when a child went missing or somewhere else, they could get expert advice. Secondly, somewhere where there was a child protection ethos; that if something was happening in

29 October 2013 Mr Jim Gamble

a particular Facebook environment or elsewhere, someone could go and take an immediate look at it. I am working with the Isle of Man police at the minute and looking at how they can integrate their digital strategy both on and offline that allows them, in a recognised form, to patrol for their citizens online. Rather than say, “Do not report crime to us”, say, “You can engage this Twitter patrol and you can ask it questions and it will give you professional answers and help you, because it can be in your pocket”; looking at how you do that. That opportunity has been missed.

I think Keith Bristow is an outstanding police leader; I think Peter Davies has had a very difficult job to do. A lot of people left CEOP. I hear all the time that the numbers are much bigger now and that is great if they have been able to do that on a budget that is largely the same, of £6.4 million in their annual review. If they have done that by reallocating, fantastic, but when I was there and I gave evidence to Home Affairs Select Committee the week I resigned, we took a headcount of who we had. It is about 120 now. I know they say then it was 86. I am a bit concerned about the difference.

I read with interest the phrases used, because I think everything here is “more resources and number of people available for CEOP’s work”. What does that mean: number of resources and people available? How many people do you think are in CEOP right now? How many people do you think are working right now for child protection in the country? If I were you that is the question I would want to know. I also understand that you have heard about the psychological support that staff get. Let us look at psychological. How many staff are in CEOP today, working for CEOP, that have had psychological support? That will give you an idea of the true number who are working directly for CEOP; those people who have had that psychological support who are working in child protection today.

You have to get beneath the rhetoric of “there are more”. Apparently, there is 145. Apparently, it is 175. If “access to resources” means that they can use Serious Organised or National Crime Agency resources, are they the right resources? In my experience in education, I came in as a hard-core police officer. I did not come in thinking, “Well, we will go down this education road”, but over the six-year period what I saw was, “Educate and empower young people. They can protect each other. Educate and empower those who are in a role to protect them. Support social care. Support teachers. You will have a far greater opportunity of target-hardening those people who are vulnerable while you do it”. I get no sense that that has been captured.

When we talked about statistics of children rescued, we defined a child protected as someone who—if you are a paedophile and you are engaging two children, we would count those two children because we would know the name of the social worker, the name of the paedophile and the law enforcement officer engaged. In the broader safeguarding, we would not, if you were a martial arts instructor that held a whole load of classes, count 130 children because we had arrested you. We would count those children that you may

potentially have engaged with. You have to look at statistics and say, “Are we improving? Are we getting better? Where have all these things gone?”

You can bring someone in from the National Crime Agency who is a grade six analyst and put them on a desk to look at child abuse images. Is that what you want or do you want someone with a child protection background who specialises in that and who has built a history in doing it to be looking at that; who will consider not just the issues about viewing the images and the trauma and that, but some of the other evidential issues and some of the safeguarding issues? I said at the time I would love to be coming back to say I had been proved wrong. I am not being malicious or malign when I say that I think I have been absolutely proved right. The brand has been diminished and diluted. The operational independence, do you get a sense that CEOP is operationally independent of the National Crime Agency? It is not even independent of politics and the Home Secretary. That is not a good place for child protection to be. If you were a safeguarding board, I think you would be heading for trouble.

Q121 Tracey Crouch: I apologise for having to whizz off straight after the question. My mother was a social worker in Children & Families for many years. I have to say I thought I was pretty immune from stories about child abuse, but some of the statistics that we have been hearing I have found quite distressing. You talk about the role of linking up the agencies for child protection. Do you think that our current flock of social workers are being adequately trained to deal with this kind of abuse on the internet and how can we improve, not just awareness among our enforcement agencies, but within our protection agencies as well?

Jim Gamble: That is a great question. I am chair in Hackney. What you have there is a blended staff. We talk about the frustration and the problems. You have young staff who grew up with Bebo, then MySpace, then Facebook, who use Instagram every day. Those young social workers bring a skillset with them that the older ones do not have, but what the older ones have is experience of dealing with families living in complex situations, facing issues around alcohol misuse, mental health and all the other safeguarding issues that are there.

Do I think that the training is good enough? No, I think it could be improved. Do I think we are in a dire situation? No, I do not. My eldest daughter is a special needs teacher. She is 28. She grew up with Bebo. So in the classroom she understands all those issues. My son who lives and works in London, when his younger sister was coming of age he was the one who did not want her to go onto social networking sites. Maybe that was because he did not want her to see what he was doing, but at the end of the day it was also about protection. The youngest is training to be a social worker as we speak and so from that point of view I agree.

What I would say is we need to get this right again. The NSPCC ran a survey—I think it probably links to your question—where they said just about 50% of social workers were not confident that they would be

29 October 2013 Mr Jim Gamble

able to identify a child whose abuse had stemmed from the internet. The problem with that question was it was put the wrong way around. The question was about technology first and harm second. If you ask if a social worker could identify a child who had been the subject of neglect, abuse or mistreatment, then the statistics would have been a lot higher.

Now, there are 85,000-odd social workers on the general social work care consult register. There are about 45,000 in local authority care and about 24,000 or 25,000 delivering children's services. That survey looked at 327 or 329. Some were from the NSPCC themselves. Is it representative? I am not sure. Social workers are like the rest of us. I would think you would be *au fait*, if I am being stereotypical, with social media whereas some of the rest of us would not. Training needs to be updated and improved. It needs to be in the workplace as well. We should be delivering that training online. It has to be contemporary, because if you develop a training package now and you do not take account of the new social media sites, the new trends, the new dos and don'ts, then you lose sight of it.

It is like RIPA. I was chair of the UK Data Communications Group. The problem with the legislation is, when you make it too specific, you cannot apply it generally enough. Training needs to be about how you communicate, how you create risks.

Q122 Tracey Crouch: It goes back to your original premise right at the start about professional curiosity. Do you have any statistics or evidence or even just any suspicions as to what proportion of children who are victims of child abuse images that are posted on the internet are also on the at-risk register in terms of general protection?

Jim Gamble: No. If we go back to one of the Ofsted reports—not the last one but before—I think there was only about 12% of children who were on the Children At Risk Register who were known to authorities in any way. Those children who were dealt with, the other percentage, the adults in the house were known to create a risk.

One of the other problems is ContactPoint. How do you identify and locate a child who is subject to a risk that is being investigated by social care, by policing, by health or problems with education? ContactPoint was the mechanism by which we did that. It was scrapped on 26 August by the present Government and never replaced. That was technology that you could turn all this on its head. The former Head of Intelligence in CEOP had said to me at the time, "Look, this has made it easier and quicker for us to identify some of the children because we get partial information. You can then look for the specifics." It was seen as a Big Brother database, which it was not. Should there be better training? Yes, but I think the training needs to always concentrate on the abuse. The mechanism and means, whether it is child sexual exploitation on the street, whether it is a child being trafficked, or whether it is a child being groomed will have two things in common: people first and technology second.

Q123 Mr Leech: I do not think any of us can be in any doubt on your views as to the change from CEOP coming under the National Crime Agency but, given that it is, are there any changes that you would like to see that you think would improve the situation that have not been introduced so far?

Jim Gamble: Yes. I accept the situation as it is. If it was within my gift, I think there should be far greater engagement with the Department for Education. The education teams should be bolstered. CEOP should have absolute operational independence from the National Crime Agency, because children's voices must be heard and must come first. I am not sure how you can do that, given the present format. They will have an advisory board, but an advisory board is like an ashtray on a motorbike. It does not make a lot of difference once you start moving if people are not using it. I think they need to re-engage education much more. They need to invest in education.

They could still do what I have suggested around creating special constables who would work regionally with their local police forces for £1.4 million. Recruit, train, and accredit through CEOP, attached to the National Crime Agency. None of that would be stopped, but I think they also need to take a step back and learn the lessons about brand. Taking down signs, changing the CEOP website to put under it "A command of the National Crime Agency", that is not the spirit of children first. That is evidence of the organisational ego of the larger diminishing the presence of the smaller simply because the larger is now new and wants to create a profile.

I would put the CEOP media team back in CEOP, not integrate it into the NCA. If you are going to be "children first", then you need to be advocating and saying to the NCA, "No, you are wrong. We are going to take on these cases. We are going to do it in this way and we are going to invest this amount of our budget in education". I do not believe that that can happen.

Q124 Mr Leech: Does the NCA offer anything to CEOP?

Jim Gamble: Yes, it offers a capability around technology when it comes to in-depth investigations into the likes of the onion router, but the NCA should have been a good and active partner of CEOP. I believe the NCA as an entity is an excellent idea. As far back as 2001, when I joined the National Crime Squad as an assistant chief constable, the director general said to me after three months, "What would you change if you could?" I said, "I would drop the 's' and put an 'a' on it and make it the National Crime Agency and consolidate resources around organised crime within it". Now, the fact of the matter is it is a good idea, but putting things like CEOP in it will force CEOP, as it has done, to submit to its image, not allow CEOP to thrive as an independent environment. How many people are looking for missing children now? That is a CEOP responsibility. How many people do you think in CEOP are working on missing children? The Prime Minister was asked on Channel 5, on the news programme, how many people he thought were searching for images. I know when they put to him "between two and five" he was shocked.

29 October 2013 Mr Jim Gamble

The fact of the matter is, if you want to see the real difference you need to get into CEOP and you need to ask some questions because, as far as I am aware, everything that I have said to you is absolutely true. If you accept everything I have said to you as true and you are not deeply concerned, then there is a huge issue.

National Crime Agency is great. Organised crime, terrorism, money laundering, fantastic. Child protection in Hackney, child protection in Northumbria, child protection in Humberside, that is about local child protection teams, local safeguarding boards, local police. It is about how you support them, about how you create materials that go into their schools. A national hub that had teachers in it, that had social workers in it, that had those people that create those imaginative products that children can engage with in the classroom so that they learn the importance of friendship and supporting a friend who is being bullied online, who are able to work through real life cases to say, "If that had been one of my friends, I would have wanted them to report. Who would you report to?"

You can be scared of your own shadow in this game, because nobody wants to attack any of the big social media providers. I will not name the charity, but I heard someone from a charity who is on the advisory body to one of the social media organisations that has just changed its default settings for 13 to 18-year-olds say, "We will need to learn more about it". I think, "Well, if you are learning more about it after the fact, you are not an advisory body, if your advice was not being taken before the fact". What can I say? The National Crime Entity is a great entity but subsuming CEOP into it is a recipe for disaster. You can bring however many people you want in, but while they are still working there do you honestly think they are going to come in and say, "No, I do not think it is a good thing"? Do you think that will be career-enhancing or career-inhibiting?

Chair: It is 1pm. We had better draw this to a halt. Jim, thank you very much.

Jim Gamble: Thank you.

Tuesday 19 November 2013

Members present:

Mr John Whittingdale (Chair)

Mr Ben Bradshaw
Angie Bray
Conor Burns
Tracey Crouch

Paul Farrelly
Jim Sheridan
Mr Gerry Sutcliffe

Examination of Witnesses

Witnesses: **Simon Milner**, Policy Director, UK and Ireland, Facebook, and **Sinéad McSweeney**, Director, Public Policy, EMEA, Twitter International Company, gave evidence.

Q125 Chair: This is the further session of the Committee's inquiry into online safety and we have three panels this morning and I would like to welcome our first witnesses, Simon Milner, the Policy Director of Facebook, and Sinéad McSweeney, the Director of Public Policy at Twitter.

Q126 Tracey Crouch: Good morning. I will start by asking if you could outline what it is that you already do to prevent harmful or illegal material online.

Sinéad McSweeney: In terms of illegal content we have a zero tolerance for any child sexual exploitation material on the platform. So when that is reported to us, we review those accounts. They are suspended and they are, in addition, reported to the National Center for Missing and Exploited Children in the US and they then have channels of communication with the relevant law enforcement agencies, who can take action both on the offenders but also ensure that if there is a child at risk, that they can be identified, located and rescued as well. We also have relationships with law enforcement and police in different countries. So we have good working relationships with the police here in the UK not only so that they are aware of our processes and procedures in order to request information of us and work with us, but also so that we would participate in some education and awareness raising with them about how the platform works and how to contact us when they need to, whether that is in an emergency or when they are investigating crime.

Q127 Tracey Crouch: What about harmful content, before I move to Simon?

Sinéad McSweeney: Yes. Sorry, did you say Simon?

Tracey Crouch: No, no.

Sinéad McSweeney: Okay. In terms of content generally, clearly, there are rules as to the type of content that is allowed on the platform. So when content is reported to us that is in breach of our rules, we take action on those accounts. In addition, because there is such a diverse range of discussions and contact that take place on the platform, we also have built into the product the ability for users to label the media that they may be uploading as sensitive, and the default setting for every user is that they do not see sensitive media without a warning.

Q128 Tracey Crouch: You do not have a report abuse button though, do you?

Sinéad McSweeney: We do, we do.

Tracey Crouch: Okay.

Sinéad McSweeney: We have it within each tweet because Twitter is built around the small bursts of information that are tweets. But right within each tweet there is a report button and once the user hits that, it takes them to the range of possible issues that they may be reporting, whether that is abusive behaviour, impersonation or illegal content.

Tracey Crouch: Okay. Simon?

Simon Milner: From our own perspective, we also have a zero tolerance approach towards both illegal and harmful material. On the illegal side, as well as having clear policies about what people can and cannot use our platform for, we also use technology. So there was much talk yesterday in terms of the announcements made at the PM Summit around technology. We use one of the pieces of technology that people are talking about, photo DNA, a piece of technology created by Microsoft, and we use that to scan every photo uploaded to Facebook. That are some 350 million photos a day against a database of known images of child exploitation imagery, and we will not allow those to be uploaded and will take action against those accounts, including notifying the authorities about them. Then we work closely with CEOP in respect of their access to that data via Netmec in order to track down the offenders. When it comes to harmful material, that is pretty much very hard to spot by technology so that is where our reporting processes come in, and we too have extensive reporting processes via both our Help Centre, which anybody can access—they do not have to have a Facebook account for that—or from individual pieces of content. They can report it to us or indeed report it to somebody else who can help that user take action so, particularly, in the areas, for instance, of bullying and harassment, we do not tolerate that. Those reporting processes are incredibly useful to someone either who themselves is feeling a risk of harm or if somebody sees somebody else on the platform who they think is at risk, then they can use those reporting processes.

Q129 Tracey Crouch: This week, as I am sure you are aware, is anti-bullying week and there has been a great deal of discussion about cyber bullying over the past few months, especially as a consequence of some rather tragic events. What are you doing to work with

19 November 2013 Simon Milner and Sinéad McSweeney

organisations to try to raise awareness about cyber bullying in particular?

Simon Milner: So perhaps if I take that one first. We work with a number of anti-bullying organisations. Indeed, yesterday, I was at an event in London with 450 schoolchildren and their teachers with the Diana Award. The Diana Award has an anti-bullying work stream and they have a fantastic champion there in a young man called Alex Holmes. He does great work around the UK, working with schoolchildren, enabling them to become anti-bullying champions so we support that work. We help to fund what they do and I was there yesterday to talk mainly to teachers to help them understand how to deal with these issues on Facebook, because it is something that we absolutely recognise they need help with. But we also provide lots of help via other people who reach out to schools. So Childnet are another great charity for doing this, because we recognise bullying typically does not just happen on one platform and will happen across a range of different media as well as in the school. Therefore, working with people who can not only talk to the schools about Facebook but also about Twitter, about Snapchat, about Ask.fm and other services that young people are using is much more effective than having Facebook necessarily coming to the schools.

Sinéad McSweeney: I think we would have a similar approach in terms of partnering with the people who are talking to children all the time in this space, so the South West Grid for Learning, the UK Safer Internet Centre, participating not just in the Safer Internet Day or the anti-bullying weeks but on an ongoing basis, highlighting the resources that are available both within the platform and more generally in terms of breaking down the advice that we have to ensure it is suitable for each different category of people who need to know and understand what is happening. So, for example, in our Safety Centre we would have tips for teachers, tips for parents, tips for teens, recognising that the language and the context may need to be slightly different for each audience. That is material that we have highlighted again, as I say, to organisations who are working in this space on a daily basis, whether it is Parent Zone or BeatBullying or whatever, so that they can link to our material and also so that we can link to their material so that there is a constant shared learning. Also, as Simon says, recognising that the context for the behaviour that you may be seeing on one platform may be behaviour and activity that is occurring in other platforms and also in the offline world, it also about encouraging how to deal with online conflict, encouraging empathy and also trying to educate young people that the consequences of their online behaviour are the same as offline. If you say something online, it has an impact on somebody in the real world although for young people it is their real world, so sometimes we have to be careful even in terms of that kind of language. But it is a question of ensuring that we are using our own communication channel effectively by working with people like the Safer Internet Centre on their Connect with Respect campaign but then also getting into the other worlds in which young people are accessing information and ensuring that those who are guiding them through the world, whether it is their

teachers or parents, are as equipped to deal with the questions and activities that they are involved in as the young people themselves.

Q130 Tracey Crouch: You both mentioned that quite often harmful behaviour is happening across multiple platforms. Do you think that all social media providers are equally good at dealing with this or do you think some are better than others? I have in mind, obviously, the controversy that came out over the summer about Ask.fm and I just wondered what your views are on that. Do you think that that, perhaps, poor or lacklustre response from Ask.fm had a very negative impact on the wider social media providers?

Sinéad McSweeney: I think we can only speak for our own platforms but I know that our experience, whether it is ourselves and Facebook who are here today, is that it is an area that we work on together. We are not territorial or proprietary about the way in which we work with young people to ensure their safety online. We all participate together in, for example, the planning day for next year's Safer Internet Centre and there is another planning day coming up in December. So, from our point of view, it is about sharing the expertise and ensuring that together we are giving young people the skills and resources they need.

Simon Milner: In fact, we work so closely that when Sinéad and her colleagues recruited our Head of Safety for Europe, we were genuinely pleased. We thought this was good for her in terms of her development but also good that Twitter sees the value in having somebody who has been working on safety for four years come and become part of their team. I think that we have to recognise one of the things about young people is they love new services and they love to try them out. Usually, they are the first ones to adopt new services. It would be unrealistic to expect that those new services have invested to the extent that our two companies have in safety. Nonetheless, I think we have a duty as citizens but also as part of this industry to help them, so that is what we try to do. I certainly do that around, for instance, the UKCCIS Board that I sit on. We are always trying to share intelligence around what are young people using and how can we help them to be well-educated in using those services.

Q131 Tracey Crouch: How many people do you employ to combat illegal or harmful content?

Simon Milner: We have a user operations team of several hundred people. It is not a public number. I am afraid I cannot tell you. Our company as a whole has 5,500 people. We have several hundred people who work in user operations, including hundreds of safety experts, so we have people who have seen everything before and know how best to deal with it. We are always also looking to work with outside organisations to try to ensure that we are consistently learning about what is the best way of helping our users.

Sinéad McSweeney: Similarly, we are a much smaller company obviously. We have 2,000 employees worldwide. We have trust and safety teams based in San Francisco and also here in Europe in Dublin, so

19 November 2013 Simon Milner and Sinéad McSweeney

those teams are providing 24/7 coverage right across the globe across the different time zones. The trust and safety and user services teams are divided into sub-teams to address the different issues that can arise across the platform, the different rule breaches. There is a team looking at abusive behaviour or user safety behaviour through to impersonation through to illegal content. So those teams are covering, as I say, the different time zones on a 24/7 basis.

Q132 Tracey Crouch: Final question, Mr Chairman. Clearly, although you might like to think so, neither of your platforms are perfect in dealing with particularly harmful content. What do you think you can do better to try to stop or prevent future harmful content, because I recognise that illegal is very different and probably being dealt with quite well?

Simon Milner: That is a really tough question. I would say we never rest on our laurels. We are always looking to innovate and I think the moment when we start to think we have this cracked, it would be an unfortunate moment. It certainly would not fit with the culture of the organisation, which is to constantly innovate. So I really would be reluctant to predict what is the next best thing we could do but I would be very surprised if I came back here in a year's time and said, "We are just doing the same as we did last year". We are always looking to innovate.

Sinéad McSweeney: I think like anything in life, there is always the potential to do something more effectively, more efficiently and in a better way for users. I spent 10 years working in police communications and in that context, of course, you also in some ways have the division between what was illegal and things like antisocial behaviour, which was harmful. So it is about constantly working with the community, and in our case that is our users, to know and understand how they want the platform to be a safer and better place because at the end of the day, it is there to enrich their lives. It is connecting people to events and information and news and so on.

Q133 Tracey Crouch: But you both recognise that you still have weaknesses?

Sinéad McSweeney: It is a question of understanding that as the technology evolves, just like in the world of crime or antisocial behaviour, people think of new ways to breach your rules so you have to ensure that you are one step ahead. So we have a dedicated engineering team on the trust and safety side constantly alive to the possibility that there are issues within the product that we will need to address when somebody finds a new way of using the platform. So I do not think anybody would ever put their hand up and say, "We are done on safety", and particularly not when it involves children.

Q134 Chair: You said you each have lots of people sitting there who are safety experts. If I push the report abuse button, how long before somebody looks at what I am reporting?

Simon Milner: In Facebook, it would depend frankly on who you are and what you are reporting. So if you were reporting that somebody you know is suicidal, we are going to look at that very, very quickly. It

could be within minutes. If you were reporting that there is some spam that you are seeing, we may not get to that for a week so it would depend on the seriousness of the harm that you are reporting. Also, frankly, how old you are. So teenage reports we are going to look at more quickly than we do others. But one of the things we always hesitate is to make those hard-and-fast rules because, otherwise, we might find that people think, "I have this problem. I will report myself as being suicidal because that means I will get looked at sooner". So we always aim to get to reports within 48 hours and most of them we do that. As I say, for those that are most serious we will get to them very quickly.

Sinéad McSweeney: Similarly, depending on the nature of the abuse or harm that is being reported. Again, threats of self-harm, suicide, threats of violence and anything under child sexual exploitation category is looked at within a very short period of time. Again, other issues may take longer.

Chair: Are we talking minutes again?

Sinéad McSweeney: It can depend. It could be a minute to an hour. Again, you cannot be hard-and-fast in terms of the issues but we do respond to those first, before other issues.

Chair: For instance, there is a choice. If I press the report abuse button, I am given the choice of different categories?

Simon Milner: Yes.

Sinéad McSweeney: Yes.

Q135 Chair: I see, and depending which I choose will determine how long it takes to get back to me?

Simon Milner: It could be that but, also, it may be dependent on what is going on in certain events. One of the things about our teams is they are national teams so they are interested in what is going on in the news. So, for instance, around the time of the August riots 2011, the team was on high alert for content associated with those riots. So antisocial behaviour or people organising that kind of thing might not have been flagged otherwise but because we were particularly on the lookout for that, then we will deploy more resources. So it will depend on the circumstances, the public circumstances as well as the circumstances of the individual who is reporting.

Q136 Angie Bray: In terms of antisocial behaviour, the debate has also moved on to whether you should be showing certain footage of things like beheadings, which I think, probably, just showing that does cross into what I would consider to be fairly abusive. I know that Facebook has taken quite a strong line on that. Has it Facebook's view changed as this debate has raged or are you still adamant that this is freedom of information and people should be allowed to see these?

Simon Milner: I think the way I would put it is that we have refined our approach to this kind of content. I am sure we are grateful every day is that we live in a country where beheadings are abnormal, where random acts of violence do not happen to most people we know, but there are lots of people who are using our platform in countries where this is a normal part of life. They want to use our platform to highlight

19 November 2013 Simon Milner and Sinéad McSweeney

what is going on in their neighbourhood, in their country, in their city. Sometimes that means posting graphic content because that is the only way to get the world's attention. We recognise there is a place for graphic content when people are condemning it, so absolutely not to glorify it and not to take pleasure in it. When people are using our platform to condemn this and to bring the world's attention to it, then we should be able to do that. However, we also recognise that given that we are a platform that also has young people, people under 18, we need to enable people to get more prior warning and we are taking steps to ensure that people share responsibly. There are different ways in which we can do that on the platform and we are developing those, frankly, in the light of some recent events. So you are right to highlight it and I am glad I have had the opportunity to address it, but it is something where we are refining our approach because we think there is a place for people to share that kind of content in the right context and with appropriate warnings.

Q137 Angie Bray: But do you set the context? It is one thing to show footage but you are not suggesting, are you, "We are showing this because it is demonstrating what terrible things are happening"? You are simply showing it, so are you setting an adequate context?

Simon Milner: We are not setting any context.

Angie Bray: That may be the problem.

Simon Milner: No, just to be clear, because we do not post anything to Facebook, it is our users that post things to Facebook and it could be a government, they could be a parliamentarian, they could be a campaigning organisation and they could be an individual. An example is after the terrible bombings in Boston at the Boston Marathon, a number of people who were witnesses posted footage to say, "Oh my God, look at this horrendous thing that has happened". We enable people to do that and we enable people to share that with the world, and we think that is part of how we bring the world's attention to some horrible things that are going on. What we do is provide the tools to enable them to share responsibly and we are refining those tools as we speak to enable people to put warnings, and also to share in a way that young people are much less likely to see it. But just to be clear, if you go on to Facebook and search for beheadings, you would never have found them. Our search facility does not allow you to do that whereas if you go into many other parts of the internet and search for things like that, you can very easily find it. In the recent examples, we had no incidence of reports to us from young people or others with responsibility of looking after young people saying, "Oh, my goodness, this young person has seen this video", because it was not being shared in that way.

Q138 Angie Bray: Twitter, of course, has been under some kind of criticism for the fact that it was quite a useful vehicle during the recent terrorist outrage in Kenya where it would seem that some terrorists were using Twitter to get all sorts of messages out. Again, does that make you uncomfortable that Twitter can be used in that way?

Sinéad McSweeney: As a platform, we do not knowingly allow terrorist organisations to maintain accounts on Twitter.

Q139 Angie Bray: But were you aware that it was being used?

Sinéad McSweeney: Where we have reports to us from law enforcement, where it is brought to our attention that terrorist organisations are maintaining accounts on Twitter, we take action on those accounts. We do not allow accounts to be used for direct threats of violence or for unlawful purposes. I think the flip side of the events in Egypt, in Kenya and events right across areas of conflict is that Twitter is used by human rights activists and by the media to get information out to the world about events like those and ensure that people in real time can follow the events. But to make it clear, we do not knowingly allow terrorist organisations to maintain accounts on Twitter.

Q140 Angie Bray: But it was over a period of two or three days, not just a flash in the pan, that these terrorists were able to send out to the world what they were going to do, what they were not going to do, that they were coming again, and they were basically using it to send out their philosophical message. So at what point would Twitter have woken up to the fact that they were being used in this way? Really, the world does not need to know about that, does it?

Sinéad McSweeney: Drawing on my experience from policing and the way in which police approach the investigation of certain types of crime, there are different approaches to the existence of information in the public domain and the way in which it can assist investigation. So, as I say, we work closely with law enforcement. Where we receive reports of terrorist organisations maintaining reports on Twitter, we take the action that is required of us.

Q141 Angie Bray: Did you get any reports on that, because it was certainly all over the newspapers?

Sinéad McSweeney: I am not going to talk about individual accounts. We do not talk about anybody's individual accounts or indeed individual engagements that we have with law enforcement.

Angie Bray: So was action taken?

Sinéad McSweeney: Action was taken in those circumstances but we do not comment in detail about the interactions or communications we have with law enforcement.

Q142 Mr Sutcliffe: If I can just turn to the anti-bullying theme, in the evidence that is given to us, 30% of youngsters under 16 expect to be bullied on social media. What do you say about that? What is your view of that?

Simon Milner: I think it is sad that young people feel that. I expect if you ask them also, "Do you expect to be bullied at school?" probably a similar number would. Most bullying that we see on Facebook starts for young people in the classroom, on the school bus, in the canteen. I have spent a lot of time travelling around the UK meeting with teachers and that is a regular thing that they tell me. Indeed, because of that,

19 November 2013 Simon Milner and Sinéad McSweeney

we have allowed a feature to enable teachers to resolve issues on Facebook. They can both report things to us without having an account but, also, a young person who is feeling bullied by somebody else in school can report that person to a teacher. All they need is an email address and that teacher will get a report saying, “Simon Milner feels he is being bullied by—forgive me—Sinéad McSweeney and this is the content that he feels is bullying”.

Q143 Mr Sutcliffe: But does that happen?

Simon Milner: Roughly half of all the young people who report bullying use social reporting and that is a global number. They find it very effective for resolution. The reason we introduced this was often it was very difficult for us to understand the context of a relationship between young people and, typically, bullies are friends of those who have been bullied. Therefore, it was very hard to understand why that person felt a particular piece of content was bullying because we did not understand the wider context of their relationship, and that is why we enabled this feature for somebody who does understand that context to be able to get involved in it.

Q144 Mr Sutcliffe: Is it just teachers? One of the other things that concerns me is that children or young people are on the internet without their parents being involved. What do you do to help parents identify potential problems?

Simon Milner: I am a parent of teenagers. I absolutely understand where you are coming from although, like fellow parents, one of the things you recognise as children grow older is they do become more independent. I do think part of their digital citizenship, indeed their general citizenship, is about having an ability to be independent online, particularly around teenagers. One of the things we do provide is, firstly, parents can report to us. So if they think there is a problem on Facebook, they do not have to have a Facebook account to report to us. They can do that through the Facebook Help Centre. We provide information through Parent Zone. You mentioned the good work that Vicki Shotbolt and her team do earlier. I have done a video for Parent Zone explaining to parents about how they can deal with issues if they have concerns about what is going on on Facebook. But as with everything, including some of the things that we have discussed yesterday in the Prime Minister’s Summit, the key thing is getting young people to talk to someone. That is where we found the biggest problem in the terrible events of young people committing suicide. Typically, they have not told anybody about the problem and we cannot help somebody who does not tell us, just the same way as a teacher cannot help a pupil if they do not tell them. So that is the main message we give to parents, “For goodness sake, even if your child will not tell you, get them to tell someone who can help”.

Q145 Mr Sutcliffe: I think the point I am trying to get to, Simon, is that because we have social media, it has not suddenly become a problem. That problem has always been there, as you say, bullying at school, that sort of thing. I think that is the issue that I am

trying to get across, that you have mechanisms in place for people to get to.

Simon Milner: Also, I think one of the things that distinguishes bullying online from bullying offline is that there is a footprint. There is a record so this business of being able to report to a teacher is not saying, “Sinéad said this”. It is, “Here is what Sinéad has said to me. Here is the photo she has posted”, and that is physical evidence that can be used then to help, not to necessarily punish the bully but to help educate the bully about, “This is the consequence of what you are saying and the words that you think may be funny actually are very hurtful”.

Q146 Mr Bradshaw: Sorry, I am having trouble finding your report abuse button. Could you help us? Report abuse, where is it?

Sinéad McSweeney: It is within the tweet. If you are in a tweet the three dots indicate more content. At the bottom. It depends on which operating system you are using.

Mr Bradshaw: Don’t worry. Perhaps you can show us later.

Sinéad McSweeney: At the bottom, it says, “Report tweet”. I am happy to talk you through it.

Q147 Mr Bradshaw: It did not seem to me to be in an obvious place. You said earlier that you felt you did respond in a timely and effective fashion to reports of abusive tweets but that was not the experience of our colleague Stella Creasy and the woman who was involved in the save a woman’s face on the British bank note campaign. They are quite high-profile people so how can we have confidence—they were very unhappy about how this particular issue was responded to and the abuse they suffered—that ordinary people who do not have that level of profile and voice are having their reports taken seriously and dealt with quickly enough?

Sinéad McSweeney: I think without getting into too much detail of individual accounts—I appreciate that while Ms Creasy has given evidence in public here that Ms Criado-Perez, while she has spoken publicly, has not given evidence in this forum—in some ways, what was experienced in that number of days in August is not the commonplace normal experience of a Twitter user. The levels of activity that were directed at those individuals were unprecedented in my time with Twitter, so that is the first thing to mention. Since then we have done a lot of work to highlight the reporting resources that are there because part of the issue was accessing the reporting forums. It was not a case of non-responsiveness to our report. I think the issue that they were talking about was the ability to report so the in-tweet reporting, greater ease of access around forums, better tools for users are things that we have improved since and continue to improve, going back to the other member’s question, that that job is not done.

We have increased the resourcing around our trust and safety team. Simon already made reference to the person we have recruited to head up user safety for Europe and she has started on our team since then. In addition to that, again, we are working with the organisations in this space like South West Grid for

19 November 2013 Simon Milner and Sinéad McSweeney

Learning, UK Safer Internet Centre, so that when people contact them about issues, they immediately are able to give them the advice and the resources that they need. But publicly at the time there were a number of statements from Twitter about what happened and the fact that we took on board the responses that we received. I have spoken personally on numerous occasions in the time since to the people involved in that and I continue to take on board the feedback they have.

Q148 Mr Bradshaw: You mentioned the South West Grid for Learning as part of the UK Safer Internet Centre—in fact, both of you have more than once—and in your evidence you have been full of praise for this organisation. How important do you think their role is in helping to mediate and report abusive comments and getting them taken down?

Simon Milner: I think they are particularly helpful for schools so there are professional hotlines. They are there mainly for teachers and they can help people understand problems because they have seen them before and, particularly, Laura Higgins, who runs the helpline there—it is a shame you are coming to the end of your evidence, she would be a great person to bring in to talk about it—she is an expert in all the different services that young people are using and she has seen every different kind of issue in the school before. I was with her yesterday at this event with the young people and their teachers and not one of those teachers had heard of her helpline, so it was a great opportunity for her to tell them about it and it is wonderful for me to have this opportunity to tell people about her helpline. They have a phone number that teachers can call and say, “We have this problem. Can you help us?” Then what she has is a hotline to us. Often she can help people resolve their problems without needing to come to Facebook but sometimes she cannot. She has a hotline to our team in Dublin to help resolve things where she cannot do it.

Sinéad McSweeney: That is the same approach that we have, that we ensure that she has all the information she requires and in the situations where she cannot in the moment resolve the issue that the school is bringing to her, she can contact us and we give her the additional information she requires.

Q149 Mr Bradshaw: I should perhaps declare an interest, Mr Chairman, because she is a constituent of mine. Given the high praise that you both have for her and her organisation, is it not surprising that it is run on a shoestring funded by the European Union?

Simon Milner: Indeed, I was talking with her about this yesterday. We have provided some resources to help her and her colleague David Wright run a road show around the country, so we helped to support that. But I think you are right in saying this is something that we as an industry should look at, as Laura is looking to develop that helpline, as in, “Can we help her further, including giving additional resources?” It is a good point to raise.

Sinéad McSweeney: Similarly, we have assisted them with training workshops for hotline managers and so on, so we have been asked and have been able to

contribute to the way in which they provide their service.

Q150 Mr Bradshaw: But this valuable service, I think, is being done by one and a half people with very little money. It is running out next year. You have deep pockets. Is this not the kind of thing that you should be funding as a matter of course?

Simon Milner: Laura has not actually asked us for money to do that yet but I am sure when she does, possibly as a result of this, we shall be listening with a very open mind.

Q151 Paul Farrelly: You are both global businesses so, presumably, you share with each other in your organisations experiences from around the world.

Simon Milner: Yes.

Paul Farrelly: Presumably, if something happens in one part of the world, as with any big global organisation, if you are approached by the press or committees like this, you will have notes on how to deal with questions?

Simon Milner: I will not put it as strongly as that. We tend to talk about what are the issues we think might come up and, frankly, who is going to answer the question first.

Q152 Paul Farrelly: Sinéad, if you were asked about things that are happening in one part of the world, would you expect to be briefed by an organisation?

Sinéad McSweeney: It depends. My responsibility goes beyond the UK so I would be familiar with issues that are going on in the EMEA region, which is Europe/Middle East basically.

Q153 Paul Farrelly: Okay. I was following the build-up to the All Blacks match at the weekend and, as we were doing this inquiry, I was asked whether we have come across the case that is causing huge controversy in New Zealand called the Roast Busters. Have you come across that case?

Simon Milner: No, I was at the recent Family Online Safety Institute conference in Washington DC with NetSafe, the New Zealand equivalent of the UK Safer Internet Centre, and they did not mention it, so I am not aware of that, I am afraid.

Q154 Paul Farrelly: Have you come across it?

Sinéad McSweeney: I am not familiar with it.

Q155 Paul Farrelly: No. I am just reading from a CNN report and reports have been all over New Zealand press over the last two weeks so this is from a couple of weeks ago. Just a synopsis of this case, it is about a group of teenage boys who were boasting online about raping drunk and underage girls, getting so incoherent they did not know what they were doing. What came to light, which was exposed by a Channel 3 television programme in New Zealand, was that for some months they have had a Facebook site on which they were posting these boasts. Days after the exposure of the site, it was shut down and there was apparently another site that had started on Facebook. Facebook is not the only social medium to be used by this gang. Just again from the CNN reports,

19 November 2013 Simon Milner and Sinéad McSweeney

Twitter was also a conduit for their boasts, Ask.fm and also YouTube. I clearly cannot ask you what lessons you are currently learning from that experience because you do not know about it.

Simon Milner: Mr Farrelly, I am not aware of that case. I am happy to ask my colleague, who does my equivalent role in that part of the world, about it and see whether there are some lessons we might learn. I do not really want to comment further. It is clearly not appropriate because I do not know any more about it.

Q156 Paul Farrelly: Would you both drop us a note on it?

Simon Milner: Sure.

Q157 Conor Burns: Can I just ask in relation to this report abuse facility within Twitter, does it alarm you that you have three relatively sophisticated and regular tweeters on the Committee and we cannot find it? I was not aware that it existed. When did you launch it?

Sinéad McSweeney: It was rolled out at the end of July and the plan was to roll it out across all the platforms by Christmas but, in fact, we achieved that by the end of September. If you are saying to me that we need to highlight it more, that is something that I can take away. We have done blog posts. We have tweeted about it. We have spoken to various safety organisations who work in this space. I think every time that I have been at a meeting, I have mentioned it but as I know only too well, having spent 10 years in Comms, that you can never tell people something often enough so we will keep telling people about it.

Q158 Conor Burns: I think the message from us is that with the nature of what we do, we are probably slightly more prone to abuse sometimes than your average user and I was not aware that it existed.

Sinéad McSweeney: It is not the only means by which you can report abuse. You can also report abuse through the Help Centre.

Conor Burns: I know. I have just googled that. I have seen that there is another mechanism to do that.

Sinéad McSweeney: Yes.

Q159 Conor Burns: Facebook. When we were in California, I raised an instance where someone had posted something that was profoundly libellous against someone else. It was reported and absolutely nothing happened. Facebook came back and said they deemed that it was legitimate comment. Would you like to comment on that?

Simon Milner: I do not know the details of the individual case but, as you can see, we looked into it and we do not always agree with reports that we get. Frankly, a lot of the reports we get are frivolous. The classic one is somebody says they like Justin Bieber and other people report them as being suicidal so I am not belittling it but we have looked at it.

Q160 Conor Burns: What about somebody saying that they believe somebody else is a child abuser?

Simon Milner: Again, we will look at the context and because one of the things we have learnt is just because somebody has said it, that this is suicidal or

child abuse, does not mean it is. We have to look at the context and the details.

Q161 Conor Burns: No, I am putting to you that when somebody posts that they believe somebody else to be a child abuser and that was not taken off.

Simon Milner: I do not know the circumstances to the individual case, and perhaps you and I can correspond on it afterwards, but one of the key things that is open to people if they think we have made the wrong decision is they can go to the courts.

Conor Burns: Which is out of reach for a lot of people.

Simon Milner: That is a matter for Parliament as to how the defamation process works in the United Kingdom. I do not think that is a matter for me.

Q162 Conor Burns: But there are often instances where there are lovely, warm words that come forward about procedures, hundreds of people on help desk, but we encounter real people who are finding that there are no options open to them and you hide behind, "That is a matter for Parliament". But you are the publishers. You are allowing these things to be published and said about other people.

Simon Milner: We are a platform for free expression. We have a mechanism for somebody to report to us something that they think is defamatory or libellous. We look at those very carefully, we are risk-averse as a company, so I am sure that the team that have made that decision have done so with full knowledge that having made that decision to leave that content up that things are open to an individual to not only take action against the person who posted it but also against us. But on the matter of, "These are warm words", these are not just warm words. We see examples week in week out of particularly young people and people in distress being helped as a result of reports by their friends—young people who are reporting that they are feeling suicidal or indeed that they have taken some pills or cut themselves. In situations where we see that somebody who thinks somebody is in imminent risk of harm, we will alert the local law enforcement who would go and find that person. Quite typically, they would get to them before they do the deed or in order to help them so we help people in the real world enormously week in week out.

Q163 Conor Burns: Yet, as a publishing platform, you allow comments to remain up that a newspaper would not in 100 years dream of publishing.

Simon Milner: I do not think that is fair in the context of I do not know the details of this case but I am absolutely certain that a team would have properly looked at that and made the decision based on the available evidence in the context. It is open to that individual to take action if they wish.

Q164 Chair: Can I pursue with you some of the measures that you have in place? First of all, what is the minimum age for somebody to subscribe either to Facebook or Twitter?

Simon Milner: It is 13 for Facebook.

Chair: 13.

19 November 2013 Simon Milner and Sinéad McSweeney

Sinéad McSweeney: Yes, our services are not directed at under-13s.

Q165 Chair: 13, and how do you verify that somebody is 13?

Simon Milner: With our platform, when people sign up for Facebook, there is quite an extensive new user process and one of the things we require people to do is provide their date of birth. If somebody puts in a date of birth that is under 13, we will not allow them to open an account and we will also use technology to prevent them from trying to put in a new age from the same device, trying to change their age, so that is one mechanism. We recognise that people, unfortunately, lie about their age. Did you see this recent report from the NSPCC, which came out on Friday, about this? They reported a pattern that we have seen in other studies that in the majority of cases of 11 and 12-year-olds joining Facebook, their parents have helped them set up the account so the parent knows that their child has a Facebook account. One imagines typically the deal is, "You can have a Facebook account but you will be my friend on Facebook so I can look after you". In those situations, it is very difficult for Facebook to spot that that person is an underage user. We still also encourage and indeed find reports from our users of underage accounts incredibly helpful and indeed when teachers ask me about this, I say, "You can report it. You can let us know that somebody is underage".

Q166 Chair: Okay and what about on Twitter?

Sinéad McSweeney: We do not collect age information on sign-up. I think Twitter has established a reputation in the area of privacy. We minimise the amount of information that we require from users to sign up so we do not collect age or gender or other details about our users. Where it comes to our attention that somebody under the age of 13 is using the platform, their accounts are removed.

Q167 Chair: You say you have to be 13 to use Twitter but you are also saying you do not ask anybody if they are 13 or over 13?

Sinéad McSweeney: Yes. That is a balancing between the premium that we put on our users' privacy and the issues that you are raising.

Q168 Chair: How does somebody know they have to be 13?

Sinéad McSweeney: Sorry?

Chair: If I joined Twitter, am I told that, "You have to be 13"? How do you make people aware?

Sinéad McSweeney: It is in our privacy policy that this service is not directed at people who are under 13.

Q169 Chair: So you have to go into your privacy policy and read it and then you discover that you are supposed to be 13?

Sinéad McSweeney: Yes.

Q170 Chair: Right, okay. What about fake identities, people who open accounts in false names?

Simon Milner: With Facebook, that is against our rules. You have to use your real name on Facebook

and, indeed, we think that is the core of Facebook's success. We would not have reached 1.2 billion monthly active users had we not have that policy because Facebook is all about connecting with people you know in the real world. So it is against our terms and we very much encourage people if they see somebody who they think is not using their real name, they are an imposter, to tell us about it and we will then look into those accounts and remove them if we conclude that is the case. We may require people to prove their identity if they claim that this name that appears very fake is real. That is something that we take seriously and indeed is at the heart of our mission.

Sinéad McSweeney: We do not require users to use their real name. Most people do because they want other people to be able to find them and connect with them on the platform. We allow people to use pseudonyms. We allow people to set up parody accounts that range from emergency cute puppy accounts through to political satire. More importantly, we have seen the platform used in areas of conflict by human rights activists, journalists, people who are at risk of harm from the information that they are attempting to get out into the world publically. That is very important to us and that is why we facilitate that kind of political activism and content on the platform.

Chair: As I understand it if I set up as Donald Duck there is no problem with Twitter.

Tracey Crouch: That has already been taken.

Chair: Donald Duck the 52nd. Twitter, you are perfectly content. Facebook, it is only if somebody tells you that I am not Donald Duck and then you will do something.

Simon Milner: No, it is not if somebody tells us they are not Donald Duck, it is if somebody else tells us.

Chair: Yes, I understand.

Simon Milner: There are also certain names that we will look out for so you cannot set yourself up as David Beckham, for instance. We also, like Twitter, provide a process for people to have their accounts verified. This is particularly useful for people in Government, for instance, so you know that when you look at David Cameron's page on Facebook it is David Cameron and not somebody pretending to be David Cameron. That is something that we are rolling out to help people who are public figures to ensure that people understand yes, this is the real person.

Q171 Chair: Let us assume Donald Duck⁵² indulges in highly offensive behaviour, trolling or even posting child sex images, how do you identify them? Do you keep records and ISP addresses?

Simon Milner: If somebody is using our platform to try and distribute child abuse imagery then that is going to be spotted through photo DNA assuming it is a known image. As you may be aware, we are working together with other technology companies to try and ensure that we share even more intelligence around these known images.

Chair: I am asking how you identify whose account it is.

Simon Milner: Reports are incredibly powerful. We kind of have a neighbourhood watch community of

19 November 2013 Simon Milner and Sinéad McSweeney

scale, and our users really care about their safety and the safety of others in the platform. They will be reported to us and then we will deal with it.

Q172 Chair: That does not address my question. It may be important to you, you may find it but if it is being posted by somebody who claims to be Donald Duck52, how would you identify it in that instance?

Simon Milner: I see, I am sorry. In the situations where, for instance, law enforcement are on to somebody like that and they want to find out who they are and where they are living and what have you, we have a process for them to request communications data from us to enable them to do that. That would include the IP address.

Chair: You will be storing the IP addresses and the messages for how long?

Simon Milner: We store the IP logs for a period. I would have to come back to you to tell you exactly how long. The messages, it will depend. Typically it depends on how long a person wants to retain those messages but most of the time law enforcement will have the messages because somebody has come to them saying, "Look at this thing on my account". They have the messages, they have the content, what they need to know is who is this person and that is when they can come to us to ask for the communications data.

Chair: Twitter, do you keep that same data?

Sinéad McSweeney: Yes, we also retain communications data. We have protocols and guidelines for law enforcement on how they can work with us to request information, and they can also request that we preserve information pending receipt of further requests from them.

Q173 Chair: But you are keeping records of tweets and IP addresses from where they originate.

Sinéad McSweeney: The tweets are public anyway.

Chair: They might get removed or deleted.

Sinéad McSweeney: In the main most of the activity is public and remains public, and we will retain a certain amount of communications information.

Chair: You retain IP addresses?

Sinéad McSweeney: Yes, we retain communications data.

Q174 Chair: You would allow law enforcement access to that with a court order, would you?

Sinéad McSweeney: We receive law enforcement requests. They range from emergency situations where if there is an immediate threat of life we respond to it straight away, and also in other areas of serious crime we deal with requests from law enforcement on a case by case basis.

Chair: Civil actions?

Sinéad McSweeney: Civil actions, again it would depend on circumstances. It is difficult to talk about hypotheticals but on receipt of valid legal process we deal with those requests.

Chair: I would need to get a court order.

Sinéad McSweeney: Yes.

Q175 Chair: A court order from the UK, would you accept that?

Sinéad McSweeney: Again it is not my exact area of expertise the actual legal process that is required. I would need to come to you on that but we would need valid legal process.

Chair: It was suggested to me you had to get a court order in California, which is not always terribly easy for a civil action for say privacy invasion or defamation.

Sinéad McSweeney: Yes, but there are various treaties and so on that cover civil litigation and co-operation between jurisdictions also that would be invoked in those circumstances.

Chair: I think my colleagues have exhausted their questions so thank you very much.

Simon Milner: Thank you very much.

Sinéad McSweeney: Thank you.

Examination of Witnesses

Witnesses: **Tony Close**, Director of Content Standards, Licensing and Enforcement, Ofcom, **Claudio Pollack**, Group Director, Content Consumer and External Affairs Group, Ofcom, gave evidence.

Chair: For our second session this morning may I welcome Tony Close and Claudio Pollack both representing Ofcom?

Q176 Tracey Crouch: Could you perhaps just start by telling us what regulatory powers you do have in relation to the internet, please?

Claudio Pollack: Yes, our role is limited to television and television like content broadcast over the internet in the UK, originating from the UK. We do not have any powers that go beyond that, the regulation of content.

Q177 Tracey Crouch: That would include video content for example, child abuse videos or rape

pornography, or something like that? That would include that?

Tony Close: If that content was included in a regulated service. If it was included in a linear television service provided over the internet or if it was included in an on demand service provided over the internet and established in the UK, yes, it would include any content.

Tracey Crouch: But if somebody posted up a homemade video, for example, this would not be included within your regulatory powers?

Tony Close: Probably not, no. Not if it is not part of a broader regulated offering, a broader service is regulated.

19 November 2013 Tony Close and Claudio Pollack

Q178 Tracey Crouch: Given the extent of Ofcom's powers and the obvious expansion over time as technology has changed, do you think there will be a greater role for Ofcom in the future regulating internet content?

Claudio Pollack: Shall I take this one? I think at the moment there are a mix of instruments around making the internet safer for people. There may or may not be a different role for us in the future, and that is obviously a matter for Parliament. What I would say though is that the mechanism that exists today, the long established mechanism that exists today for the regulation of television services, which has been very effective, I do not think it would be appropriate or possible to extend that form of regulation across all of the content on the open internet. I think a different mix of instruments will be required over time to make the internet safer for those people that use it.

Q179 Tracey Crouch: You do have people working at Ofcom on harmful and illegal content on the linear platforms that you were talking about?

Tony Close: Yes.

Tracey Crouch: How many people do you have working on it?

Tony Close: Within the standards enforcement team within Ofcom we have around 40 people but I think if you included some of the other teams within Ofcom that have a role in monitoring, researching or developing policy around potentially harmful content, it would be around 50 people. They, of course, work on a range of different content related issues at any one time.

Q180 Tracey Crouch: If your powers are extended into wider internet use, perhaps like draft Communications Bill at the moment in front of the House, do you foresee any problems with Ofcom having further powers or wider powers to do with this issue?

Claudio Pollack: It really depends what it is that that extension means.

Q181 Tracey Crouch: Given obviously this inquiry has been looking at harmful and illegal content on the internet, and yet you by far the most powerful regulator on these matters in general terms for television and radio do not have any regulatory powers, do you think that it is time that you did and that you were able to help in terms of regulating content in a way that is obviously very much needed?

Claudio Pollack: I wonder if it is worth saying a little bit about how we carry out protection on television and radio services and then maybe we can explore whether there are aspects of that that would be appropriate or relevant in the open internet.

Tony Close: Yes, I think it is worthwhile reflecting just quickly on that. We do have powers in this area. They are limited by statute. They do require us to regulate linear television or on demand services when provided over the internet as well as via other mediums or platforms.

Chair: This is what you delegate to ATVOD?

Tony Close: In relation to video on demand, yes. Across those services that we currently regulate on the

internet we have a comprehensive set of rules. We are required in relation to video on demand with ATVOD to implement those rules. We continuously monitor compliance with those rules through complaints or proactive monitoring. We refresh those rules where we think that the industry has moved on or public policy concerns have moved on. We have very significant powers currently to either fine providers who have broken the rules or to stop or to suspend their services online or not online. So we have a comprehensive set of powers and a comprehensive set of rules that apply to these services even when provided over the internet already. I think the challenge is identifying the best aspects of the way Ofcom currently operates and identifying the best aspects of the existing framework and seeing how they could be applied to a broader set of services potentially online.

They are obviously limited by geography, our powers, and there is a significant challenge around regulating content over the internet that comes from outside the EU of course.

Claudio Pollack: For example it is not possible at the moment, as I understand it, to broadcast in the United Kingdom without a licence that is granted across Europe. On the open internet content can come from anywhere in the world. of course.

Q182 Tracey Crouch: The on demand services, so the XXX channels for example that are broadcast on Freeview, presumably if, for example, they have specific licensed agreement that they can only provide programmes after midnight or something, if they were to bring that forward to 10.00pm that is where you would step in and remind them of their duties?

Tony Close: Yes, in relation to both linear and on demand adult services, services providing pornography that are regulated by Ofcom and by ATVOD as well there is a broad range of interventions and measures based on time, based on preventing access to children, double, triple PINs and obstacles for gaining access. Obviously there are limits on the content as well that are already in place, limiting the explicitness in particular environments. For example, you cannot have hardcore pornography on Freeview even behind considerable PIN and other access restrictions.

Q183 Chair: In terms of what is and what is not possible, there has been a lot of press speculation about the need to have greater control over the internet and I suspect a lot of it simply is not possible but one of the things that particularly you have looked at in a different context is website blocking, URL blocking particularly. When you last looked at that you threw up a whole lot of technical reasons why it was very difficult to do. Is that still the case in your view?

Claudio Pollack: We looked at it in the context of online copyright infringement and whether website blocking could play a role in that. We absolutely did highlight a number of technical challenges and limitations but for me the report was very clear in saying that, to making it more generic and applicable, if this about lessening the availability of content that is considered harmful, harmful in different ways, that

19 November 2013 Tony Close and Claudio Pollack

website blocking can play an important role in that. It is not the answer to everything. It is not 100%. It is not watertight. It can be bypassed and it is not perfect in the sense that, given the amount of content out there, it can over block. It could block things that you did not mean to block and it can under block, it can allow certain things through.

In both of these examples, public policy examples, if you take blocking or filtering as part of a suite of measures then it absolutely can have an impact and can play a role.

Q184 Chair: It can play a role but if I am a technologically literate child abuser seeking to overcome technical measures, can I do so?

Claudio Pollack: I am hesitating because the conversation I was having was focused more on content that is generally lawful but accessed by children that we do not want children to access. If we are talking about illegal content, for example child abuse content access on the internet that is slightly further outside our area of expertise. The simple answer is at the moment, yes, my understanding is that there are technologies in place that allow those that wish to access these images to bypass controls that are put in place.

Chair: We are told that a lot of this material is now lurking in the dark net as they call it, Tor is particularly identified. Is it your understanding that is something that it is possible to intercept and identify or is it so hidden that it cannot be reached?

Claudio Pollack: I think we are reaching the limits of our expertise in terms of what Ofcom does. We are far more focused, as I say, on understanding how people can be protected or protect their children from content that they do not want to be viewed in terms of this aspect, these two aspects of child protection. Tony, your turn.

Tony Close: The only thing I would add—and Claudio is right, this is outside our remit—there have been some limited but notable examples recently of prosecutions or investigations of people using Tor or other dark web browsers and routers. It is possible and it has happened on very limited occasions.

Claudio Pollack: It is obviously a big, big area of focus for CEOP, as was, and the IWF. When I have met with them we have explored and also assisted with some of the technology expertise that exists within Ofcom in understanding the mechanisms around identification and blocking. There will be, given the current state of technology, imperfect mechanisms but I suspect they have a very strong role in law enforcement as well.

Q185 Chair: In terms of the role Ofcom plays therefore in encouraging the provision of child protection filters and that kind of thing, how much power do you have to lean on the ISPs for instance?

Claudio Pollack: Beyond the areas of broadcast and on demand content on the internet, our role is not about powers. We do not have any powers to mandate or in particular we do not even have a function, I would say, to engage with internet service providers. The real legal route and where our remit fits here is around our media literacy duties. It is very much

about understanding and encouraging media literacy among, in this case, children and parents, and we will carry out a lot of research and therefore be the keeper of the facts. I would add that as part of that role, our main role on online safety, we have a seat on the executive board of UKCCIS, which is the main institution that leads activity in this area. As part of theirs and the Prime Minister's negotiation or agreement with the main internet service providers to provide network level filtering by the end of the year, they have asked us to carry out a particular role in understanding how that implementation goes.

Tony Close: Shall I add something to that? Before talking about the specific reports that we are carrying out into parental views of online behaviour and safety, it is worthwhile just making absolutely clear that in our role as a board member of UKCCIS we provide all of the data that we harvest as part of our media literacy programmes so that public policy can be developed, public debate can be had about the risks and benefits of the internet and of child internet use. Claudio touched upon some reports that we will be doing over the next year for the Government around child internet safety.

Next month we hope we will be reporting to Government on parental awareness of, take up of and confidence in parental controls and other strategies, mediation strategies, available for parents to protect their children in an online environment. We will be following that up in one year's time with a follow up report to look at how things have progressed. Just quickly in between the two reports we will be producing a third report for the Government that looks at progress made by the four major ISPs in implementing network level filtering.

Q186 Chair: You say you do not really have much control over the ISPs, that your main area is TV companies and radio, but the Government has said that it wants to ensure that internet enabled devices are supplied with filters and that you are going to be involved in overseeing this. What does that mean?

Tony Close: I think it is what I was just talking about. I do not think we have a specific role.

Chair: But this suggests that you are going to have one in the future.

Tony Close: I think that that is just another way of saying that at least for the next year we will provide a number of reports that provides the Government with our insights into how network level filters have been implemented, whether or not ISPs have delivered on the promises. More than that they will provide our insights on how parents feel about the level of protections that are available to them and whether or not they are confident or not confident in protecting their children in an online environment.

Chair: You see Ofcom's role essentially as one of research and opinion surveys.

Claudio Pollack: Within the current statute that is exactly right. Beyond the areas that we have identified and described, there is no regulation of the internet in this country in the statute and we do not have a role in that nor do we have a role, a formal role in policing or mandating filtering. The conversations that happened were all about a voluntary commitment to

19 November 2013 Tony Close and Claudio Pollack

deliver a form of network level filtering and Ofcom, because of its media literacy duties and because of its expertise in networks, has been called upon by the Government to help in a degree of evaluation of the extent to which the filters have been properly introduced and also the impact that that is having on the way that parents and children use the internet.

Q187 Chair: But you do have a role in licensing telecoms companies, do you not?

Claudio Pollack: We have. I was going to say that when you said we only do television and radio that is in terms of protection of UK citizens from harmful content on radio, television and TV like content on the internet. Separately, of course, we have a role around the regulation of telecommunications companies as providers of electronic communications, networks and services. It is not through a licensing regime, it is through a general authorisation regime but that explicitly does not cover regulation of the content that is delivered by those networks.

Q188 Chair: It does not but if the Government chose to say, "We are now going to make it a requirement that you also have child protection measures", you could do that?

Claudio Pollack: Yes. To be very clear, what we are describing is what our role is within the existing statute. Of course there could be a different role if the statute was changed but that is obviously a matter for Parliament, not for us.

Chair: That would require primary legislation to change the terms of the regulatory regime for telecoms.

Claudio Pollack: I believe so, yes.

Q189 Mr Sutcliffe: Just on that theme, I think you are pointing out you are a regulator without powers in terms of this area and clearly that is a decision for us as Parliamentarians to make, but I think your point us to a direction. What concerns me then is if the ISPs know that you do not have any regulatory powers what is your relationship like with them in terms of how are you seen by the ISPs in this sort of area? Do they work with you in a proactive way or do you have to react to what the agenda is? I am trying to get a feel really in terms of what the relationship is like without you having the powers to be able to say to them, "You must do this, that or the other".

Tony Close: I wonder if I might answer first in relation to the specific task we have ahead of us in the next year, and whether Claudio may want to add anything about our broader relationship. We are conscious that because we are limited by statute that we do not have specific powers to require ISPs to do certain things for us in order for us to carry out a process of reporting to Government on network and filtering. As part of the agreement with Government on doing this work, we secured agreement that the Government would contact the major ISPs themselves and ask them to co-operate with us in order for us to deliver this set of reports. I think we all agree that it is important and we cannot do it without the co-operation of the ISPs. We have no broader role

with ISPs but, Claudio, I wonder whether you want to add anything?

Claudio Pollack: I have a lot of experience in dealing with the internet service providers in those areas where we do have power and that is a particular type of relationship as you would expect. In this area it is quite straightforward. We do not have any powers but nor do we have any duties or functions so there is not a gap if you see what I mean. Where we would be coming in and saying, "There is a problem here in terms of what we are expected to deliver", would be if there is a gap between our duties and our powers to deliver that.

To be very clear, the provision by the four largest ISPs of network level filters to be used by parents by the end of this year was an agreement between the Prime Minister and the internet service providers. That agreement is about what they deliver but also as part of that agreement and in the exchange that we have it must be that they are required to co-operate in any form of evaluation of whether they have delivered to what is essentially a voluntary deal. If there is not co-operation, for example if we find that it has not been implemented properly or substantively or there is not co-operation in our ability to carry out that task then of course it is an agreement between the Government and the ISPs and it is for the Government to decide, if this voluntary arrangement has not delivered what it hoped to deliver, whether it wants to consider other avenues as well. At the moment it is a voluntary agreement in which we are assisting.

Q190 Mr Sutcliffe: Tony, to go back to the survey, I think, you are doing of parents, this report on parental involvement, which I am pretty keen on because I think that part of the problem is that parents do not know what is going on in their own households. How do you go about it? What are the terms of reference? What is the background to it?

Tony Close: You are going to have to forgive me if I cannot provide you with full details of this because I am the guy at Ofcom that looks after setting rules and enforcing those rules. I am not the guy that looks after the quite complex and comprehensive programme of research that we do but I will have a stab at answering. Claudio, you might want to follow up.

We carry out a range of different quantitative and qualitative pieces of work. We are doing them on an ongoing basis so that we can benchmark and track changes in parental attitudes. The qualitative pieces are obviously limited in terms of numbers of people that we talk to but really gets under the skin of parents' and teens' attitudes to internet use, online safety, what concerns them or worries or distresses them, what they like about it, what they understand about parental controls. The quantitative piece is obviously different. It is bigger, it is less detailed but tries to canvass a significant range of views and attitudes to what the risks are online, what steps parents take to mediate or mitigate those risks, what strategies that they develop. It is quite comprehensive. I cannot go through all of it.

Q191 Mr Sutcliffe: I think somewhere in the report it talks about there is evidence now that people are

19 November 2013 Tony Close and Claudio Pollack

more aware of what the issues are because of experience, if you like, online. How often are these reports commissioned? How often are the surveys changed?

Tony Close: Okay, one of the reasons the Government were probably keen for us to do the work is because they are aware that we already do this on an annual basis as part of our media literacy programme. Those two reports, and there are other reports, programmes of work that we carry out as well that might feed into this are a rolling programme of work. I cannot tell you how long we have been carrying them out for but I think it is a considerable period of time.

Claudio Pollack: I think it is since 2005, so annual surveys since 2005.

Mr Sutcliffe: There is an opportunity now to see a pattern of things happening.

Tony Close: Yes. It enables us to track people's behaviours and attitudes as their internet experience changes, as they become more confident or as they become less confident, as they become more aware of risk or less aware of risk.

Mr Sutcliffe: I do not know whether it is feasible, Chairman, but it might be worthwhile getting a copy of the sort of questions that are asked of parents, if that is possible.

Claudio Pollack: Under the media literacy duty every year we have a research report, a very, very comprehensive research report one on adult media use and attitude and one on children and parent media use and attitude. It is the primary source, as Tony said, used by UKCCIS to understand changes and it is absolutely vital in understanding how things are moving in this area, with limitations. There are a number of things that it shows around attitudes. One of them is that most parents are doing something, there is a number of things they could do, but most parents are also reporting some difficulty in using certain tools. No majority is using, for example, filtering but a combination of using filters, being in the room when the child is using the internet, talking to their children once a month, the combination of those three mechanisms is 85%. So 15% are doing nothing, but within that 85% there are a number of people that are doing just one or just two of those things.

The other thing that I think is fascinating—and, yes, we will absolutely share the questions of what we are doing annually—is the specific targeted report that we have been commissioned to do using that data. What makes this area so difficult is just how quickly it moves. One thing that I am going to quote to is if parents were saying and taking comfort from the fact that the PC was in the room that they were in and they could observe what was happening, in just 12 months tablet computer use at home among five to 15-year-olds between 2012 and 2013 has gone up from 14% to 42%, and that gives you a real sense of the challenge of protecting children. Even when parents are investing the time and effort to do so, it is very difficult because things move so quickly. There is a lot in the research that will help understand that better.

Tony Close: Just very quickly, Chairman, of course we will share the questions with you and we will share the report once we have finished it as well.

Q192 Chair: Just to be clear, the Government has waved sticks at Google, at Microsoft and at the ISPs. The Prime Minister has basically said, "Report back to me within so many months" with the implicit threat that unless they do these things action is going to be taken against them. The position is that at the moment there are not any powers to take action.

Claudio Pollack: Sorry, say that again?

Chair: The powers do not exist at present to take action.

Claudio Pollack: In the area of regulating internet service providers in having a role in policing content the powers do not exist today. Of course if there are individuals who have the capacity to introduce legislation then they have a different response.

Chair: Of course, but therefore the Prime Minister and Ministers' implicit threats are that they will have to introduce new legislation to take powers to require internet companies to do these.

Claudio Pollack: Yes, that is right.

Q193 Chair: You do not have at the moment really any provision within the licensing requirements that would cover this kind of area?

Claudio Pollack: There is nothing. It is the general conditions of entitlement that is through legislation that derives from Europe around electronic communications. Not only is there nothing in the general conditions nor do we have the capacity to introduce regulation that is around content using that instrument.

Q194 Chair: Television like material is covered by ATVOD?

Tony Close: Yes. The powers are vested in Ofcom. Ofcom contract out the function of regulating television like video on demand services to our co-regulator, ATVOD.

Chair: Would that cover YouTube?

Tony Close: It would cover parts of YouTube. YouTube is a mix of services. It is in large part and most notable for user generated content and hosting user generated content but increasingly it is a platform for professional services provided from different corporate entities. There are a number of professional YouTube channels that are established in the UK that meet the definition of a television like service and are regulated by Ofcom and ATVOD.

Claudio Pollack: To be clear, in order to be regulated they both have to be TV like and they have to be established in the UK. Content that is visible on the internet that is neither TV like nor established in the UK, we would not have jurisdiction.

Q195 Chair: But if I post a video on YouTube that I filmed on my handheld camcorder or whatever, is that covered by ATVOD?

Tony Close: No, probably not, not if it is user generated content and it is just a part of broader offering. It will be covered by YouTube's own community standards.

Q196 Chair: Sure, so how do you draw a line between YouTube content that is covered and YouTube content that is not covered?

19 November 2013 Tony Close and Claudio Pollack

Tony Close: Partly on terms of jurisdiction, to put them on to the site you have to be established in the UK.

Chair: All right, so assume we are in the UK.

Tony Close: Then you have to identify a service that exists, something that you can see, feel, something that is whole, and then you have to run through a series of potential criteria or characteristics to determine whether or not it is TV like or whether or not its principal purpose is the provision of TV like material to consumers. This statute, I think, contains a number of conditions, all of which need to be passed in order for us to determine, or ATVOD in the first instance, if something should be subject to regulation.

Q197 Chair: Do you feel that this whole area needs further Parliamentary examination, because I was involved in the Bill that set up Ofcom and none of these services existed at that time?

Tony Close: I think it is fair to say that there is a challenge. There are different degrees of protection

offered for different types of service online, very comprehensive rules set for linear services online, less comprehensive rules set for television like on demand services, and no statutory rule set or intervention for certain other types of material. There is a challenge there. It is a legitimate debate to be had about whether that is an ideal scenario for consumers or whether or not we should be thinking about a more coherent framework for media standards that spans a greater set of audio visual media. I think there are certainly some benefits in thinking about that.

Q198 Chair: Will this feature in the Communications Bill, do you think?

Claudio Pollack: You have someone giving evidence shortly that I think would be better able to answer.

Chair: Indeed, and that is a question we might put to him. I think that is all we have, thank you.

Claudio Pollack: Thank you very much.

Tony Close: Thank you.

Examination of Witnesses

Witnesses: **Rt Hon Damian Green MP**, Minister of State for Policing, Criminal Justice and Victims, **Mr Edward Vaizey MP**, Parliamentary Under-Secretary of State for Culture, Communications and Creative Industries, and **Claire Perry MP**, Special Adviser to the Prime Minister on Preventing the Commercialisation and Sexualisation of Childhood, gave evidence.

Q199 Chair: Good morning, thank you for attending our third panel this morning. It is afternoon now. May I welcome Damian Green, the Minister of State for Policing and Criminal Justice from the Home Office, Ed Vaizey, Minister for Creative Industries and Communications, and Claire Perry, the Special Adviser to the Prime Minister on Preventing the Commercialisation and Sexualisation of Childhood? We have just been having a discussion with Ofcom about what powers are available to them should ISPs and other internet involved companies not voluntarily adopt some of the measures that we have been encouraging them to take, to which the answer was there were very little powers. Do you think we need to give Ofcom more powers in this area?

Mr Vaizey: We await your guidance, Chairman, on who you would like to answer.

Chair: I think possibly, Mr Vaizey, you are best placed.

Mr Vaizey: I knew I should not have said anything. I think Ofcom obviously has some powers in this area. It is clearly a regulator of broadcast services and co-regulates what we call video on demand with the Association of Television and Video On Demand. Anything that is a broadcast like service that is broadcast over the web, Ofcom has the powers to regulate. As you know, it has also been asked by the Secretary of State to report on parental awareness and how comfortable parents are with the safeguards that are now being put in place. They were also behind creating ParentPort as a one stop shop to allow parents to get the kind of guidance they need. We are working, related back to video on demand, on common media standards because we take the view that as television and internet services converge anyone, parents,

consumers of any kind, will assume that the same standards apply to what appears on their living room screen, which I think you can still call a television for these purposes.

Ofcom also sits on the UKCCIS Board so they have a great amount of input into what we are doing in this area. I would be open to any discussion on an extension of their powers. I have taken the view that we can achieve a lot without necessarily imposing legislation or widely extending Ofcom's powers at the moment, for example the whole issue of filters where we, I think, have made some rapid progress, has been by engaging in a dialogue with the ISPs. Self regulation, if I can put it that way, seems to me a way of making the kind of rapid progress one needs, not only just rapid progress but also keeping the flexibility so that we can react quickly to events. Some of the changes that Google have made, for example, would not necessarily have succeeded, I think, as quickly if we had had endless debates about the appropriate legislation and so on.

But it is quite clear that Ofcom has a role in this space. The key issue, I think, will be always to be open to ideas and suggestions about whether or not Ofcom should have its powers extended and if so how, what its remit will be, particularly considering you are dealing with global companies who effectively deal with different regulations all across not just Europe but across the globe. I do not know whether Claire wants to add anything to that?

Claire Perry: Thank you. The independent parliamentary inquiry that I chaired raised the issue that there are numerous regulators in this space and I, like the Minister, think it is an interesting and valid question as to whether Ofcom's remit should be

19 November 2013 Rt Hon Damian Green MP, Edward Vaizey MP and Claire Perry MP

extended. The two areas where, I think, the issue most arises is one around to whom does one complain if one has problems around content or treatment, and of course ParentPort is a good attempt to try to centralise the complainant process. Perhaps more work could and should be done around publicising that. Indeed we will move onto the internet safety campaign that is being funded by the ISPs. One of the asks is to direct parents where to go, users where to go, when there is a problem.

I think it is right and good that Ofcom has been given an implementation role in the roll out of the policy around filter adoption. One of the questions on the filter process is what does success look like? With a sense of about 30% of the households in the country being those with children one might argue that is a good, soft target though there are not, of course, official targets for this. Asking Ofcom to look at the implementation of that and also perhaps to distinguish between ISPs and the success of their implementation is a very valid thing to do.

Like the Minister I am very minded to think that if we were trying to regulate such a fast moving space in any form we would still be sitting round looking for parliamentary time on the first debate on filtering implementation. Instead of which we have extraordinarily effective and dynamic filter roll out, and indeed companies are competing to offer their customers the best filters and the most family friendly packages. I think an extended role is possible, and I welcome the Minister's commitment to looking potentially at how that could look.

Q200 Chair: The whole thrust of the pressure that has been placed on internet companies to date has been rather, "Unless you agree to do this then the Government will make sure you have to do it". Do you see any advantage perhaps, and we have a Communications Bill coming, in the Government taking powers rather as the Government took powers in the Digital Economy Act to require ISPs to do something if they failed to do it voluntarily?

Mr Vaizey: As I say I am open to any suggestions and I am looking forward to the Select Committee's report. I think one has to be careful. If one took too wide a reserve power, if I can put it that way, to "regulate the internet" that would create an element of uncertainty. Businesses need certainty and need to know what regulations they would be required to comply with. We need to know what problem needs to be fixed and why legislation rather than working with organisations and encouraging them would be the answer. As you say, Mr Chairman, I do think that the potential of legislation, and the Prime Minister made that clear on a number of issues in terms of his speech in July and continuing dialogue he has with the industry, is always there.

My message to all the companies in this space is that there is potentially an appetite in Parliament for regulation and that they should not be blind to that and therefore co-operation—and to use a terrible American expression—getting ahead of the curve is a much better place for them to be but they must understand that is, as it were, the mood in Parliament that I don't think MPs would shy away from

legislation should they feel that they were not getting the adequate results that they needed.

Claire Perry: Mr Chairman, just on that point, if I may challenge you slightly, sir. The idea that companies are doing this or else I think perhaps is something that we felt a couple of years ago. I may just be starry-eyed through lack of sleep after yesterday but I genuinely think that the growth of corporate social responsibility among those who are making their living from anything to do with internet activity is really quite impressive. Certainly the British ISPs are well ahead of the ask in terms of delivering and, with yesterday announcements, we can see that some of the global internet companies who perhaps dance to a very different legislative tune have also woken up to that. So again perhaps we are in an awakening of a new dawn of social responsibility on the web, which is to be welcomed, but I would perhaps slightly challenge that the companies are living in fear of regulation. I think we are beyond that point.

Q201 Chair: That is encouraging. Can I turn to the illegal material because that is particularly going to be I suspect more for the Home Office. The area of data retention in order to identify perpetrators of distribution of child abuse images and so on, that strays into what has been a difficult territory for the Government in recent months. Are you satisfied that enough data is being retained and is available to the police to identify people?

Damian Green: I think in this instance it is not a problem of data retention because the civil liberties aspect of the debate does not pertain here. If people are producing, exchanging, storing child abuse images then they are committing a serious criminal act. So, as I say, both legally and morally it does not seem to me that whatever civil libertarian arguments one may wish to adduce about data retention in other spheres apply in this case. I think the key is identifying the images, blocking them, trying to get into some of the more hidden networks, moving on peer-to-peer exchange and so on. Those are the areas where activity both by the industry and by this Government, and indeed Governments overseas with whom we act in concert, is concentrated.

Q202 Chair: Are you getting complete co-operation from every single internet service provider for instance?

Damian Green: In a sense this is more a matter for search engines than ISPs and obviously it is both because the ISPs will host the sites. One of the parts of yesterday's announcement after the Prime Minister's summit, was that Google and Microsoft have changed their algorithms so that they can now both identify and block child abuse images. People are using search terms, 100,000 search terms and more, so they now have a dynamic algorithm that will be much more effective than original ideas of just producing search terms and saying block all of those. People who both produce and search for child abuse images are not only evil, they are cunning and it does not take much cunning to decide to change a search term slightly. So you do need the full extent of the technological

19 November 2013 Rt Hon Damian Green MP, Edward Vaizey MP and Claire Perry MP

expertise that is available to companies like Google and Microsoft to ensure that the algorithms can cope with that. The tests that the Child Exploitation Online Protection Centre and other bodies have been running show that these are very effective, what is coming in. Perhaps most encouragingly we learnt from Google yesterday that instead of getting back a child abuse image, getting back a warning page saying, "What you are seeking may well be illegal and do not do this" essentially, that has already reduced the amount of searching by 20%. So it has had a very significant immediate effect.

Q203 Chair: Obviously the progress that has been made through search engines is welcome but a lot of the distribution of material that is being done by the hard core is not going to be done using search engines. Do you think enough has been done and to what extent can you assess the scale of the distribution that is occurring either through peer-to-peer networks or through the dark net?

Damian Green: You are absolutely right, Mr Chairman, there are three elements to it. There is the blocking of the initial search, which we should not dismiss because what it will do is stop people embarking on this particularly horrible journey so it is worth doing in its own right. But you are right, people who are hardened may well be using peer-to-peer or may well indeed, for the worst type of abuse images, now be using now the dark net, in the current jargon. The answer to your question is yes in both those areas. One of the other things we announced yesterday was a pilot project that CEOP, along with the Internet Watch Foundation and the industry companies will be working on to see how we can deal with peer-to-peer. That is obviously different from using a search engine algorithm for reasons the Committee will understand. So that is one project. One of the key areas where the UK/US taskforce, that I will coach here with an Assistant Attorney General of the American Government, will be to bring together the best industry technologists along with the best people, GCHQ and their American equivalents who are actually very good at encrypting and therefore decrypting secret networks, to use all those skills precisely to get in to the dark net and so on. So we are working on all three of those areas.

Chair: I think that probably leads neatly in to Gerry Sutcliffe's area.

Q204 Mr Sutcliffe: I do not know if Mr Green has had the opportunity to read the evidence that was given to us by the existing Chair of CEOP and the former Director of CEOP, quite opposing views about where CEOP sits. An interesting perspective from the Minister about how CEOP's role is developing and what are the strengths and what are the weaknesses?

Damian Green: The big change, I agree, having read the evidence, there was a difference in emphasis, if I can put it like that, between the former view and the current view of CEOP, is that CEOP has changed very radically over the past couple of years and has had its most radical change in the last few months by becoming an arm of the National Crime Agency. That is a game-changer for CEOP because it is not now a

small very effective, very good outfit, it is now a very effective good outfit that is part of a very large outfit. For example, the NCA will have 4,000 officers, all of whom will be trained in child protection because it has its national links, it has a border arm as well as taking over many of the international policing functions that we need in this country. It can, if you like, look the FBI in the eye and say we can now work with you as an equal, and since this is clearly a global problem it requires global solutions. The fact that CEOP itself is now part of a global size police organisation, the NCA, I think gives it opportunities and access to expertise that it did not have in the past.

Q205 Mr Sutcliffe: Regardless of others' personal views, what they were unanimous on was that there were about 50,000 potential areas where people could be convicted on internet abuse. What are the resources going to be like for CEOP in terms, and I accept what the Minister is saying in terms of being part of that bigger organisation, there may be some possibilities of it being not downgraded but diluted in terms of its ambition and in terms of where it needs to go?

Damian Green: Absolutely not. You are quite right that the CEOP threat assessment, which it inevitably has to be—it is the best guess we have that is what it is—was up to 50,000 individuals involved in exchanging child abuse images. That was this year's threat assessment. But, no, I think the exact opposite of dilution is happening. It is being amplified that CEOP now has access to people, expertise, resources, international access in a way that it did not have by itself.

Claire Perry: Just to add some colour to the point the Minister made about exchanging, the interesting behavioural factor of those engaged in this traffic is that they connect. They seek reaffirmation for their desires from connection and in a way that makes the problem easier in that if you are going after a particular node or interrupting a particular site, and we have seen this in several busts recently, you have potentially access to a large group who have connected through, even in the dark internet, a node. Mr Chairman, if I may just throw back a point about the issue of the dark net, I mean things like Tor, The Onion Router, these are often set up by Governments and indeed funded by Governments as a way of providing anonymity to people for various reasons. One thing that would be very interesting to flag up to those Government departments who are setting up these organisations is what the unintended consequences may be. Internet anonymity is both a blessing and a curse, particularly if people are using it for illegal purposes. I don't think we think enough about that when we are looking schematically at the internet.

Q206 Mr Sutcliffe: If I can just return to the regulation point with Ed and Ofcom. What was interesting this morning, Ofcom's evidence was that the regulations were not there but one can understand that for the rate of progression and rate of change that takes place. I think the negotiated route is probably the best route to be taken and it is heartening to hear that the ISPs are dealing with that. One of the things

19 November 2013 Rt Hon Damian Green MP, Edward Vaizey MP and Claire Perry MP

that I think that we need to look at is parental involvement in all of this. Again, Ofcom this morning said that they are conducting surveys of parents going back perhaps to 2005. What can the Department do or what can Government do in general terms to try and raise awareness of the potential of these issues affecting vulnerable young children?

Mr Vaizey: As I say, Ofcom was behind setting up ParentPort because it felt you needed a one-stop shop for parents to go to get all the advice they needed. The Secretary of State has asked Ofcom to report regularly, three times over the next year or so, on parental awareness. The other thing that I think has been of benefit from the negotiated route is that we have got the ISPs to agree on a marketing campaign. I took the view these are organisations that know their customers, they have to sell them services, they will know them back to front and, dare I say, each company will have pretty well paid marketing directors who should know their trade. So I think it is a massive opportunity to have the four of them work together. I know what Claire says about internet service providers competing in terms of providing services to parents, that is good because it will mean innovation, but there needs to be a strong degree of co-operation and to have them come together for a marketing campaign is a good thing. My understanding is that it is about £25 million worth of advertising that they are planning to put in place and I think next Spring is the target date. Hopefully there will be a strong and high profile campaign to make parents aware of the filters and the kind of things they can do to protect their children from inappropriate content. It is also important to say that should not be a one-off, you cannot just have a blitz once and then forget about it and assume that people will know about it for ever and a day. One has to keep refreshing and reminding parents of what issues are out there. Again Claire, who has been involved in talking to them, might have something to contribute.

Claire Perry: I think it is interesting that this question comes up as to why is this not a Government sort of public health campaign. Indeed the last Government I believe spent £3 million on the same campaign, which was called, "Zip it, block it, something it" and frankly nobody can remember what it was. It almost sank without trace I would submit, and part of the problem was it was written by us, by people who are not out there every day working at how to get marketing messages to their users. There is a collective commitment of the ISPs to do a £25 million campaign over three years to alert parents to the new filtering technology and what they can do but also the broader issue of conduct questions. Technology only solves some problems, it does solve cyber bullying, it doesn't solve sexting. There is a lot of stuff out there. I have always felt that parents on the one hand tell us that they are technologically overwhelmed and they do not understand but on the other hand are paying for these contracts. It is like, "If you do not want your children to be sexting then take their mobile phone off them and stop paying for the contract or switch the router off at night". We somehow have abrogated this space to our kids and I think it is time to remind parents that they are part of the solution as well.

I will say that one of the big breakthroughs on technology—forgive me for talking so much—is moving device level filters to the home network level is a massive step forward in making life easier for parents. The ask now for parents to install a filter on every single internet enabled device in their home is a joke. The fact that we have persuaded the ISPs to implement a home network level filter, which we were told initially could not be done for technical reasons, until TalkTalk did it, is massive because it means that parents will only have to set the safety settings once and know that everything in the home is protected. That is an enormous step forward in helping parents in my view.

Q207 Chair: Where are we on your suggestion that there should be a default setting that is a strong filter and that people should then be required to opt in to receive stronger material?

Claire Perry: Having proposed that, we of course had the Government consultation on that, which was very welcome. We heard that people were all over the place on this default on. What we have arrived at is that we are going to ask every account holder in the country, which is 20 million accounts, so this is a very significant ask, whether or not they would like to activate parental filters. Of course two thirds of them will not be parents, so they are going to be asked for something that perhaps is not relevant. We will have the box, "Would you like the filters installed?" pre-ticked. To me, in a way, that satisfies the desire to have people make a choice. We basically present them with an unavoidable choice.

Chair: Who is presenting them?

Claire Perry: I do not know who your internet account is with, but you will have an interrupt at some point in the next year and they will say, "You can now install fantastic family friendly filters would you like to come and install them?" The box will be pre-ticked, "Yes". You can't just do nothing, you have to choose to get off that page. That to me satisfied this requirement to ask people to choose, which is the classic tension. Do you ask people to choose or do you make the choice for them in quite an elegant way. It was a proposal from the industry that I felt satisfied where we wanted to go. We ask everybody and if you do nothing the filters are automatically installed or you cannot move on.

Chair: Just to be clear, one day over the course of the next year or perhaps—

Claire Perry: One year.

Chair: Right. Every single customer of every single ISP is going to turn on their computer and suddenly get a page come up saying, "Do you want filters?"

Claire Perry: To be clear, the top four ISPs who have around 85% of the market, we would like the others to commit to the same thing. They will ask you in different ways. Some might ask you when you go to query your bill online, some may interrupt your browsing session, which is a first for the UK to do that. This is the commitment that Ofcom will be monitoring. Every household will be contacted and asked whether or not they would like to switch on the filters, and the box, "Yes, please" will be pre-ticked.

19 November 2013 Rt Hon Damian Green MP, Edward Vaizey MP and Claire Perry MP

Q208 Chair: You have conducted your inquiry, you have talked about the change in attitudes of the companies who are now much more willing to pursue these kinds of things, are you pretty much satisfied that everything you wanted to see happen has happened?

Claire Perry: Well, yes and more in some ways. For example, the Google commitment yesterday, hopefully to be matched by Microsoft, to block illegal returns for search terms globally was huge. So we will basically be protecting the global internet with those changes. However, I think one can never declare victory because the technology moves on at pace, which is why regulation of the space is so difficult. I think we have a solution that is going to be what parents have been asking for, what the country's been asking for. There may be a new way of accessing the net or a new form of conduct or a new device that pops up in the next couple of years that changes again, which is why having the company self-awareness and involvement is so important. You want them to be thinking about these dangers rather than relying on politicians to constantly be jumping up and saying, "What about this?"

Q209 Chair: Given we expect more and more internet browsing to be done on mobile devices, can I check, are the mobile providers also going to be putting up this question of saying, "Do you wish to fit filters?"

Claire Perry: Interestingly, they already do that. The mobile operators had an opt in system where you had to prove you were over 18 in order to have that filter dropped. They have both expanded that, so Three has become involved and also they have moved to BBFC filtering technology, so their filters are even better and some of the issues like false positives have been removed. In a way we have layers of protection around young people now with mobile devices in the home, and of course with public wi-fi.

Q210 Chair: Damian, can I come back to the hardcore that you are concentrating on, the figure that Gerry quoted and you confirmed, up to 50,000, when we took evidence on this earlier it was suggested to us that a number of those 50,000 who can expect a knock on their door is pretty small. Is that satisfactory or should we not be deploying more resources into this?

Damian Green: Yes, and we are is the brisk answer to that question. That is one of the points of having CEOP as part of the NCA is precisely to improve our enforcement capability. You understand that that 50,000 figure is a pretty broad brush. One of the interesting things, as Claire just alluded to in another context, is that you do tend to break open groups of people, it is not a question of 50,000 isolated individuals. The successful law enforcement operations that take place, both here and overseas, have two characteristics: firstly, lots of people are involved, and, secondly, there may well be lots of people in lots of different countries. You break open networks.

One of the points made at the summit yesterday was that the big sites that are effectively child sex abuse

image multiple sites, there are probably not that many of them. There might be 10 or 12 of them based around the world and when you get the law enforcement capability to break into them you may well find very large numbers of people who are attached to them. That is in a sense the way you will get the greater number that I accept we want to see.

Chair: Jim Gamble suggested to us that you could perhaps have special constables who would receive training and then be sent out to look for this material and identify it.

Damian Green: To some extent a lot of that work, in terms of identifying where the images are and from then to the individuals is now being done more and more by the Internet Watch Foundation, and the IWF has a significant increase in its capacity coming with the extra money from the industry. The big change that will happen in the coming months is that instead of being passive and receiving information from the public the IWF will be able to go out there and actively search. The key from that will be to make those searches active, in terms of the individuals as well as the individual images. I think we are meeting this desire to have more pairs of eyeballs looking at these images and from that will flow through the information that hopefully enables us to go and finger the individuals.

Q211 Mr Bradshaw: Damian, do you know how many prosecutions there have been for threatening and abusive behaviour online?

Damian Green: I don't off the top of my head, I am sorry.

Mr Bradshaw: Would it be possible for you to let us know?

Damian Green: Certainly, yes. We will find out about that.

Q212 Mr Bradshaw: Do you think it is a serious issue?

Damian Green: Yes. It is a different part. I suppose it develops out of cyber bullying in a way, so in a sense it will be networks. Facebook is obviously the biggest one, but we have seen a lot of the other ones where this kind of behaviour has become—prevalence is the wrong word, but we have all become more aware of it simply because that is the arena in which people exchange views and information. Therefore those who are predisposed to be threatening and abusive can now be threatening and abusive online.

Q213 Mr Bradshaw: Do you think it is important that the criminal law is used as a deterrent, in terms of our learning process and how we view this sort of behaviour?

Damian Green: The principle one has to operate is that if something is illegal in the real world then it is illegal online as well. You can cause as much distress to someone by threatening behaviour online as you can offline. To that extent, yes, absolutely. There are various stages one can go through online, and just as criminals can use technology, therefore law enforcement can use technology against criminals as well. Similarly, the social networks know their audience very well, they have the capability at the first

19 November 2013 Rt Hon Damian Green MP, Edward Vaizey MP and Claire Perry MP

sign of this of enabling people to switch individuals off, to report bullying and those kind of instant buttons on screen that you can press. They seem to me to be very good trip wires. At the end you need the criminal law, but I think you need all those trip wires on the way up as well.

Q214 Mr Bradshaw: Do you think the CPS shares the seriousness with which you take this problem?

Damian Green: Yes. I think across law enforcement. The CPS will be the recipient, that is what it is for. It receives reports from the police. Again, you have to go through the procedure, the police have to know it is happening, you have to be able to collect the evidence, they have to receive complaints, they have to have people who are prepared to give evidence, all those kinds of things. If they have cases that are best resolved, as it were, at the end, as a criminal law case then they will approach the CPS.

Mr Bradshaw: I have a question for Mr Vaizey, I do not know if anyone else wants to come in before that?

Chair: Conor, do you want to come in now?

Q215 Conor Burns: I just want to ask very quickly on the social media, do you think the social media companies—Facebook, Twitter in particular—could do more than they are currently doing?

Damian Green: They are now much more aware than they were even a few months ago of the importance of that. I have been dealing with this portfolio for about four or five months and I am struck by the change throughout the industry of some of these very big companies—based and with their origins in the USA with its different tradition—where freedom of speech is such an absolute right that any kind of reduction of it is regarded with extreme suspicion. The journey that the companies, including Facebook and Twitter, have taken over the past few months is to realise that in these areas, particularly with child sex abuse where there is no argument, but also in terms of bullying and abuse that we have seen can lead to tragic incidents of teenage suicide and so on, they do now get it in a way that I suspect, until it was brought to their attention, they didn't quite.

Q216 Conor Burns: Earlier this morning when we had evidence given from Twitter we were told that there is a report abuse function now on Twitter that was brought in in the end of July. None of us on the Committee who use Twitter were aware that that had been brought in. Do you think there is more they can do to promote how to report abuse, because the reporting of abuse means it is taken more seriously if it is in volume?

Damian Green: Yes, I think that is a very good point. The timing is interesting, it was in July Twitter had got the point. All these companies have the technological capacity to solve these problems, the trick is to get them to recognise them as a problem. There is then a further problem of letting users know. I suspect in that world, once you have established something new, so much of it does get out by osmosis that people just know it. It may reflect our age that we are not instantly aware that something new is available on Twitter now, but you can guarantee that

around the world hundreds of billions of Twitter users probably do know about it now, just because that is the way things operate. But, yes, a bit of marketing to the elderly might be useful.

Claire Perry: Could I come in with a couple of points of reassurance and perhaps a suggestion? One is I had a meeting with the Solicitor General on this very issue because obviously I have attracted quite a lot of third party cases on particularly bullying or stalking and harassment issues. He may be worth taking a statement from. I was very reassured that the law has been looked at and expanded wherever necessary to include online conduct as well as offline conduct. Having been on the receiving end of quite a storm of Twitter abuse over the summer relating to my campaign, I have to say I don't think companies do do enough. I think part of the problem is the anonymity of usage.

I was encouraged with Ask.fm—having spent a lot of time with Hanna Smith's father, who was one of the young women who did indeed commit suicide—that company did set up a facility where users could choose to be anonymous, but you would know if the user was anonymous when you were exchanging information with them. People Tweet, people post abuse about how they would like to rape you and kill you because they think you do not know who they are. If there was some way of the company knowing and being prepared to verify that identity and to show you that that identity was verified I think it would lead to a diminution in that sort of behaviour. I don't think the companies do enough and there is a great concern around it, as the Minister said, given the US legal framework within which much of the global companies operate.

Q217 Mr Bradshaw: Do you think it is important that we see some prosecutions so that there is a deterrent out there?

Claire Perry: Yes, I do. I think it is deeply misogynistic as well and it was interesting over the summer because there was a bit of flurry of push back from a number of people in the public over this. I don't know that we saw prosecutions, we saw cautions and we saw apologies but prosecuting, for what is pretty vile behaviour, would be helpful.

Q218 Chair: On the point you raised, we explored this point with both Facebook and Twitter, Twitter basically told us they are perfectly happy for you to use any alias you choose and there is no requirement for you to tell them who you really are. Facebook said to us that it was their policy that you should use your real name and if somebody told them that somebody was not doing so then they might take action about it, but they would not take any action themselves to check. Are you saying that you think that those two companies should be doing some kind of verification process?

Claire Perry: I think a way around squaring the circle would be for them to indicate to other users those users that have chosen to stay anonymous. I have no issue, as I am sure many users of Facebook and Twitter do, with my identity being public because I am obviously there as a public person and I think most

19 November 2013 Rt Hon Damian Green MP, Edward Vaizey MP and Claire Perry MP

people would feel the same way. If you are aware that so and so has chosen to remain anonymous and sit behind their funny little avatar picture then it is your choice as to whether you engage with them or indeed accept communications from them. Perhaps the companies could give us the choice of who we engage with, but certainly flag up who is choosing to remain anonymous. My sense is that might start to drive down some of this abhorrent behaviour across all the social communities.

Chair: I think it was John Carr who suggested to us that Facebook should be required to verify the identity. I am not sure that is practical, but is this an area where the Government feels more could be done?

Mr Vaizey: Again, this is an area where you can work with the organisations. I certainly think there is mileage in sitting down with the social media companies.

You made the point earlier, Chairman, about the different approach of Twitter and Facebook in terms of verifying identities, and I think there are a whole range of issues that the layman would take as important in a straightforward way, "How do I report abuse? How quickly will they respond to me about the abuse? How can I challenge a decision?" If they decide that the neighbour's Facebook page saying that you are a such and such and a so and so is fair comment rather than abuse, "How do I appeal that?" Also, do the same principles apply across different social media sites? Obviously individual social media sites should have the freedom to have their own approaches, but I think there is a way of joining things up. Neelie Kroes, the Digital Commissioner, put together some safer social networking principles a few years ago. She asked some of the CEOs that work with her on those to look at them again and update them and my understanding is that they are going to come out with a statement in early 2014. It will be interesting to see that. I certainly do think there is an opportunity for the Government to broker a dialogue between different social media sites and also to examine how effective their protocols are.

Q219 Chair: As I understand it, in terms of identifying criminality the police would have to first of all obtain an order to obtain an IP address off Facebook or Twitter, you then have to go and probably get a second order in order to get the ISP to reveal whose the IP address is. Are you content that that system is sufficient?

Damian Green: It does work.

Chair: It does work?

Damian Green: As Claire said, that there were at the height of the particularly horrible trolling that is going on over the summer, people were visited and the police found out who they were and went and knocked on their door. I just observe as a fact that it is possible to identify individuals, even when they are trying to be anonymous and saying repellent things using things like Twitter.

Q220 Mr Bradshaw: Mr Vaizey, in your evidence you singled out for praise the South West Grid for Learning, part of the UK Safer Internet Centre that happens to be based in Exeter, for the work it does in

mediating reports of abuse and threatening behaviour and getting stuff taken down. I do not know whether you are aware that they run on a shoestring and the only money they get is from the European Union. I just wondered whether you thought there might be grounds for doing the same kind of thing with abusive and threatening behaviour as already happens with child abuse and there needs to be some sort of industry scheme to fund an organisation like that, and perhaps some national recognition from Government?

Mr Vaizey: Yes, I have met with the South West Grid for Learning and I am aware that they run as a lean machine and the vast majority of their funding comes from Europe. I would certainly happily look at that. That is a very good suggestion of the wider principle that the ISPs and social media sites support the work that is being done to mitigate some of the harms. The mantra is there is a huge amount of good that comes from the internet, but there is a significant degree of harm. In terms of supporting the Internet Watch Foundation and also working with CEOP, particularly into supplying skilled engineers and technicians, I will certainly look at that on your behalf.

Q221 Conor Burns: I would just like to go back to what we were talking about earlier, about the filtering. Claire, you say that people will have in the course of the next year, possibly their browsing session interrupted and you conveyed that as though that was a very good thing. In pursuing the aim of clamping down on illegal abhorrent content on line that is a good thing, but would you agree that we have to be slightly cautious that we do not step over the line into seeming to be moralising people who do wish to continue to access material that is perfectly legal whatever one's personal moral judgment about it may be?

Claire Perry: I completely agree. A big question for the ISPs was how do you get to people who most need the filters. To be clear, we know that only four out of 10 families currently employ any sort of filtering device at home. This is Ofcom data. It may have gone up slightly in the last six months, but we have a real problem in that the companies have worked quite hard to generate filters and we know that the take up is very poor. Browser interrupts is one of several ways, other companies who have a very substantial amount of online billing say that they can do it in the "my account" space. But, of course, one question is if there is a kid surfing at that time when the interrupt comes up how does that satisfy the requirement, the adults are the ones who should be putting on the filter. This is for the companies to deliver.

One of the questions, and we did test this quite heavily in focus groups, was do people mind being interrupted or being asked about filters and is it too much to ask them to unclick the "Yes, please" box, which is effectively what you are asking. The response was actually no. The analogy given was that it is a bit like slowing down for a lollypop lady, that you may not have school age children and you might be in a hurry, but because of the general question of child safety you are prepared to slow down and potentially even stop for that school crocodile to pass. Again, there has been a little bit of push back since the announcement was

19 November 2013 Rt Hon Damian Green MP, Edward Vaizey MP and Claire Perry MP

made, but not as much as one might think. I think people think it is reasonable and unobtrusive. One of the challenges was people then said, “Oh, but people will know if I have said I don’t want the filters”, which is sort of mad, because in a way they know now. The ISPs know now because you do not request to download them. There has been this sort of air of are you invading people’s privacy. Well, of course Google knows every single keystroke and every single search that everybody is conducting, so it is slightly bizarre that people are prepared to give up their anonymity to private companies who sell it and are concerned that somehow they will end up on some sort of list. There is no list, there is no Government mandate of this, this is the companies basically interacting with their customers and saying, “Would you like to download the filters? Yes, please or no, thanks”. I think it is a very valid point.

By the way, the tone of this has always been about among consenting adults not an issue, this is absolutely fine. Although of course with closing the rape pornography loophole there are some rather unpleasant areas of currently legal material that the Government rightly has decided should be illegal. Again, it does not seem to be problem so far, and I think we need to see with implementation and Ofcom’s feedback if people do think it is unreasonable, because it may be companies have to revisit how they market their products.

Q222 Chair: Can I just pursue this point, which may be best for Damian, of material that is just about legal for adults, so it is pretty hardcore but it is legal. It was pointed out to us that a successful prosecution had been brought on the basis that the material could be viewed by children. They did not have to prove that it had been, just the fact that children could view it had allowed a successful prosecution. Is that a sort of route you think could be used again?

Damian Green: As you say, it is extremely unusual and Claire has made the point about pornography depicting rape, which I think one can regard in the same way as hate speech if you like, speech that will incite violence or something like that, because that might incite criminal behaviour. The issue that I know DCMS have been dealing with is pornographic content that is entirely legal and that nobody would be disturbed, or most people would not be disturbed with adults viewing. But it is age inappropriate and the ability to stop normally young boys repeatedly and incessantly watching that kind of material is both a technical issue and a policy issue of what you should stop and where you draw the lines. It is not criminal material so it does not fall under the criminal law, but it is clearly age inappropriate for normally young boys.

Chair: I think that was the point that was put to us, which was that it could be deemed criminal under the

Obscene Publications Act if insufficient safeguards have not been put in place to prevent young people accessing it.

Mr Vaizey: It is an interesting issue. Obviously these are the points put forward by ATVOD, the Association for Television on Demand, and I think they have made some significant progress on this. As was indicated earlier by Claire, we are moving to outlaw R18 material. At the moment ATVOD can step in where sites are offering R18 material, but we want to remove any ambiguity because there is some discussion about whether one has to show that there has been harm, and obviously rape porn as well.

The question arises about the Obscene Publications Act and whether or not a website that effectively doesn’t have any mechanism for identifying the age of the user and no kind of pay wall that you have to get behind to access the material breaches the Obscene Publications Act. I am not sure it is for me to say in terms of whether sufficient prosecutions have been conducted, because that would obviously be something for the CPS. I do know that ATVOD, in a rather imaginative way, is looking at working with financial services providers and to say to them—because obviously a lot of these websites offer you free access and then hope to make you pay later—that they should not provide payment facilities for sites that do not offer robust age verification. That is issue number one.

Obviously nothing should stop us doing the right thing, in terms of prosecutions or clarifying the law. Nevertheless we do have to be aware that a lot of these sites do not provide suitable identification as to who owns them, and again ATVOD is suggesting that we clamp down on those sites by denying them their financial support. That is something we need to continue to work closely with ATVOD on, they do have a serious point. We are also in UKCCIS—the United Kingdom Council for Child Internet Safety—looking at robust age verification measures, technical measures, whether it is the unique pupil identifier that is used in schools to enable children to get access to the web, or the digital wallet that I think is a line pursued in Denmark to ensure that you can identify the age of someone by effectively giving them a digital wallet to use on the internet. I also think, and ATVOD say it in their evidence submitted to you, that there is a role for the European Union—sorry to keep coming back to Europe—of working across all these territories, because again one of the issues here is what is acceptable in this country or not acceptable in this country, in terms of culture, if you like, is acceptable in other countries across the EU. It is something we need to continue to look at and I think it is an important issue.

Chair: Thank you. I think we have exhausted the questions, thank you very much.

Written evidence

Written evidence submitted by the Children's Charities' Coalition on Internet Safety

Thank you for giving us the opportunity to submit evidence to your Committee's enquiry into:

- How best to protect minors from accessing adult content.
- Filtering out.....images of child abuse.....
- Preventing abusive or threatening comments on social media.

Our fuller views are set out in the following pages and summarised as follows:

1. Protecting children from accessing adult content on the internet can be done most effectively through educating and empowering children to look after themselves though with very young children there are obvious limits. Filtering programmes have an important supplemental role to play in supporting good practice.
2. Every internet enabled device or internet based service sold or supplied into the consumer market and likely to be owned or used by children and young people should, by default, come with protective software preinstalled and operational.
3. Law enforcement should step up its efforts to enforce the decision in *R v Perrin*.
4. Nominet should make compliance with *R v Perrin* a condition of registration. UK-based web hosting companies should be required to ensure pornography sites serving the UK have age verification.
5. CHIS supports ATVOD's call for banks and credit card companies to refuse to process payments to sites that do not comply with *R v Perrin*.
6. The BBFC should establish transparent industry standards in relation to blocking online adult content.
7. The scale on which child abuse images are now circulating on the internet, and the number of people involved in downloading or exchanging them, have outstripped the capacity of law enforcement to deal with them adequately. It is vitally important that the internet industry is enlisted to help find new or better technical solutions to combat the problem.
8. There needs to be a specific push on eliminating or reducing the number of child abuse images circulating on Peer2Peer networks and we need to invest more in victim identification work.
9. Social media sites where significant numbers of children and young people congregate should be expected to employ an appropriate number of human moderators and to deploy sophisticated software which can help moderators spot and stop bullying and grooming.
10. There is a strong case for an major enquiry into the use of anonymity or unverified identities in social media where children and young people are major users.

HOW BEST TO PROTECT MINORS FROM ACCESSING ADULT CONTENT

1. With the spread of WiFi and laptops, tablets or other mobile devices which are internet enabled it is wholly unrealistic to expect parents, teachers and carers to be able to supervise everything their children do when they go online.
2. Protecting children from accessing adult content on the internet can be done most effectively through educating and empowering children to look after themselves although with very young children there are obvious limitations to this approach. Filtering and blocking programmes can play an important supplemental role underpinning parental guidance and good practice. Such software may be especially useful supporting younger or particular groups of vulnerable children.
3. Every internet enabled device or internet based service sold or supplied into the consumer market and likely to be owned or used by children or young people should, by default, come with filtering and blocking software preinstalled and operational to provide protection against exposure to adult content. An age-verified adult ought to be able to modify the preinstalled protective programmes' settings or abandon them altogether.
4. Filtering and blocking software is still far from perfect but it continues to improve. However, any and all technically-based safety measures should only ever be seen as an adjunct to and not as a replacement for educational and awareness initiatives. Parents and children need to understand the nature of potential online hazards and appreciate both what safety software can do and what its limitations are.
5. The decision in the case of *R v Perrin* is honoured more in the breach than in the observance although it is recognised that most if not all of the offending web sites are owned by publishers based overseas.
6. The police should be more vigorous in applying *R v Perrin*, perhaps seeking to extradite overseas web site owners who make no attempt to shield minors from adult content.
7. Nominet should make compliance with *R v Perrin* a condition of operating a .uk domain name eg if a site is to publish pornography the operator must give a binding undertaking to put an effective age verification

process in place before the site goes live or within a reasonable timeframe. It should be noted that the UK's online gambling industry has used age verification with great success.

8. UK-based web hosting companies should ensure publishers making pornography available within the UK have an effective age verification process in place.

9. CHIS supports ATVOD's proposal for banks and credit card companies to refuse to process payments to any pornography sites that do not have an effective age verification process in place.

10. CHIS congratulates the UK's mobile phone networks for sustaining their policy of, by default, putting adult content behind a bar which can only be lifted by the user completing an age verification process. CHIS welcomes the recent engagement of the BBFC to oversee the administration of this scheme including setting standards governing which content should go behind the adult bar.

11. CHIS also commends the UK's largest WiFi companies for deciding that, when they are asked to provide WiFi access in a public space where children and young people will normally be present, by default they will put pornographic content behind an (immovable) adult bar. Several of the WiFi companies have already implemented this decision. CHIS calls on the remainder to make a statement making clear when they will have done the same. Smaller WiFi suppliers should follow a similar path within a reasonable timeframe.

12. The BBFC should be encouraged to develop a kitemark scheme and associated standards in respect of public WiFi and WiFi providers ought to adopt and advertise their compliance with it.

13. A child should not be prevented from accessing certain types of adult content while they are using their mobile phone company's network only to find they are able to access identical material via the same device simply by switching to WiFi. There needs to be a high degree of consistency as between the standards set by mobile operators and those being applied by WiFi providers. The BBFC would be well placed to help establish such consistency and also ensure transparency in relation to the content standards and processes being used.

14. CHIS welcomes the announcement by the UK's major ISPs of their intention to upgrade the level of protection against adult content offered to new customers and their support for the "one click" approach. The ISPs have pledged to have their new offerings in place by the end of 2013. Existing customers will be put in an equivalent position by the end of 2014.

15. Since none of the ISPs have yet disclosed what their final offerings will be CHIS does not propose to comment further at this stage other than to say CHIS believes ISPs should, as closely as possible, implement a system similar to that which exists on the mobile networks.

16. The logic of this approach points towards the need for individual accounts for each household member. By default adult content would therefore be inaccessible to the whole household and remain inaccessible unless and until a responsible adult has authorised a change, account by account. The worry otherwise is that in households with people of widely differing ages it will prove unworkable for everyone's internet access to be configured to be suitable only for a child. There are routers on the market which have been built precisely to allow for this type of arrangement. Alternatively it could be achieved on the network.

17. The BBFC once more could play a useful role in helping ISPs roll out a solution while providing consistency with other platforms and transparency as to the processes.

18. In relation to adult content not directly accessed from the internet but obtained in other ways eg via Bluetooth, USB sticks, memory card exchanges, emails, disc swaps or downloads CHIS looks to the wider deployment of technical tools to deter or deflect such activities and thereby help protect minors from age inappropriate content.

FILTERING OUT.....IMAGES OF CHILD ABUSE.....

19. The UK has done extremely well in more or less eliminating the hosting of child abuse images on UK-based web servers. The deployment of the IWF's url blocking list has also been important in limiting web access to that kind of material. Images found in Newsgroups are swiftly dealt with. However, whilst it is important to retain a strong focus on the web and Newsgroups, technology has moved on and we are now a long way from coping with more modern manifestations of the problem.

20. In 2012 the NSPCC issued FOI requests to every local police force in England and Wales asking them to state how many child abuse images they had seized in arrests made in the two years ending April, 2012. Within the NSPCC's timeframe only five forces replied but it emerged that between them they had seized over 26 million. On one calculation that would imply that over 300 million illegal images may have been seized by all forces over the same period. Numbers like these are unprecedented and while numbers do not by any means tell the full story, they most certainly tell a story.

21. On ITN News on 28th May, 2013, Peter Davies, the Head of CEOP, acknowledged that the UK police had identified between 50,000 and 60,000 individuals who appeared to have been exchanging or downloading child abuse images, principally over Peer2Peer networks. Davies said the police do not have the capacity to arrest all of these people although he said "I wish we could".

22. In no year since records began, including at the height of Operation Ore, has UK policing arrested more than 2,500 individuals for child abuse image related offences. Thus, even if there were no new offences from now on, and assuming the maximum rate of arrests was sustained year on year, conservatively the last person off the current list would not be picked up before 2032. This has worrying implications both for the abused children depicted in the images and children who may yet become victims of individuals whom the police have identified as being engaged in downloading.

23. The technology has outstripped the current capacity of UK law enforcement to cope with the volumes of images in circulation and with the numbers of offenders involved in downloading or distributing them. Most police forces around the world are in the same position.

24. However, even if the UK was living through times of super abundance, as opposed to times of austerity, it is hard to imagine how we would ever be able to manage criminal behaviour on the sort of scale indicated. Society therefore has a stark choice. Either we settle back and accept that substantial numbers of people living among us are routinely accessing child abuse images, that it has become, so to speak, part of the background music of 21st Century Britain, or we look for new and better ways to enlist the internet industry's support in finding technical measures to address the problem. CHIS does not think anyone in a position of responsibility is ready to go with the first option. We strongly favour the second.

25. There is no single measure which will get rid of child abuse images from the internet. A range of tactics are needed. CHIS puts forward the following for consideration:

- (a) Greater use of splash pages and warning messages to deter a certain class of person with a low level, opportunist or early interest in child abuse images.
- (b) Greater use of algorithms to prevent search engines being used to locate child abuse material or locate information helpful to paedophiles.
- (c) Greater use of tools capable of comparing hashes of known illegal images with images in remote storage locations and, wherever possible, in transit.
- (d) The development of botnets or other crawler technologies capable of locating images or sites of possible interest which have not yet been reported.
- (e) Establish a national initiative to give a specific focus to eliminating or at any rate hugely reducing the volume of images being exchanged over Peer2Peer networks and increasing the numbers of individuals arrested for this type of activity.
- (f) British companies should strengthen their engagement with measures designed to address the traffic in child abuse images eg by stepping up the work they do with their employees.
- (g) Ask British policing to strengthen its engagement with victim identification work and investigate if there is a case for helping to establish a strong internationally based victim identification resource.
- h. Ask British policing to construct a national database of images which will be used by all UK forces and will also integrate into Interpol's international initiative.
- (i) Mount a campaign to heighten awareness of the harms associated with this type of offending and inform people how to report online child abuse images.
- (j) Broaden participation in the UK-US Taskforce announced by the Prime Minister on 22nd July.

PREVENTING ABUSIVE OR THREATENING COMMENTS ON SOCIAL MEDIA

26. Clearly this is an area where educating people about the importance of behaving in a civilized and responsible way when using social media, and explaining the potential consequences of not doing so, will have an important part to play in combatting some of the worst excesses which have attracted the media's attention in the recent past.

27. Peer-based support networks which develop a sense of social solidarity among the users of social media, which encourage people to intervene to support someone being bullied or victimized and to bring an end to another person's bad behaviour are the sorts of initiatives which all social media sites should support.

28. However, unless social media services decide to pre-moderate every post, be it of images or text, it is difficult to imagine how they could ever "prevent" abusive or threatening comments being made.

29. Many online companies, including some small or niche social media sites, do pre-moderate everything or almost everything that goes up. They do so for a range of reasons at least one of which is a concern for their own reputation but also they are keen to minimise any potential legal liability for libel. In some instances a concern to protect younger users from possibly harmful self-disclosures has been a motivation for using pre-moderation. There may be some situations where pre-moderation is essential eg on services specifically directed at young or vulnerable children.

30. That said, the scale on which sites like Twitter and Facebook operate probably renders pre-moderation impracticable even if it was thought desirable. However, it is a myth to assume that all pre-moderation systems inevitably slow down chat or interactive environments to a point where it is impossible to maintain a sense of real time or swift action.

31. Nonetheless technological solutions are available which can analyse text streams and help identify “hot spots” connected with bullying or other types of abusive behaviour including grooming, some of which may lead on to the creation of child abuse images or sexual assaults of a different kind. The software ought to flag up potential problem areas to human moderators who should be working 24/7 and employed in sufficient numbers to be able to intervene rapidly if necessary. Measures of this type should be in place from the start of a site’s operations. Companies should not wait for a tragedy before doing the right thing. Someone in the company should sign off confirming that full consideration has been given to all child safety aspects before any new online product or service is launched, especially on to the so-called “free” internet where it is known children and young people will have ready access.

32. There seems little doubt that the ability to hide behind an apparent cloak of anonymity, in particular the ability to manufacture an entirely bogus or opaque online identity which is then used on social media sites, lies at the root of much of the problem, even on sites which ostensibly specify a “real names” policy.

33. In principle CHIS has no problem with individuals signing in as “Donald Duck III” or “Diana Dors”. There may be many situations where not using your real name will be positively helpful or beneficial. What matters is traceability. In an environment where everyone’s real world identity had been robustly verified the log in they used would be less important but one would expect people’s behaviour to improve because they would know that if they crossed particular lines police or the civil courts would be able to identify and locate them extremely quickly if required.

34. CHIS accepts that the implications of the view expressed here are major and radical. For that reason CHIS would like separate and specific detailed consideration to be given to the issue of online anonymity, perhaps focusing specifically on social media sites which are known to be particularly popular with children and young people.

35. CHIS has no desire to make it harder for whistleblowers to continue to perform an important public service. Nor does CHIS wish to require political dissidents or persons dealing with sensitive issues to disclose their true identities before they can log on to any online service.

36. However, equally, CHIS finds it difficult to accept this is a zero sum game where advances in online child protection are forever seen as being made at the price of imperilling political dissent, whistleblowing or the position of others with a genuine need for anonymity.

37. The internet is now many different things to many different people. Perhaps it is simply expecting too much for all of it to be governed by a single perspective, a single set of principles or priorities. In other words not all social media sites or online services need to be governed by the same rules. Perhaps those that are used by large numbers of children and young people could reasonably be expected to conform to different standards.

September 2013

Written evidence submitted by the NSPCC

INTRODUCTION AND SUMMARY

1. The NSPCC applauds the Culture, Media and Sport (CMS) Select Committee for launching an inquiry into Online Safety and we welcome the opportunity to respond. The NSPCC recognises the internet has brought considerable benefits to society. However, alongside these benefits, the popular use of the internet has brought unique challenges to young people and can present some significant risks to the safety of children.

2. In 2011–12 ChildLine dealt with 3,745 counselling sessions where the young person mentioned either a mobile phone or internet issue.¹ We also know from the ChildLine messaging board that negative experiences online can have a harmful impact on young people, from affecting a child’s school work to self-harm. In some of the most extreme cases, cyber-bullying in particular has resulted in young people taking their own lives.

3. Additional to these challenges, the internet has provided some adults with a new vehicle for sexually abusing children and young people—most notably, the use of some social media sites and platforms as a tool for sexual grooming and the extremely worrying proliferation of child abuse images.

4. The NSPCC believes children have a right to an abuse free experience online and that Government, industry, the voluntary sector and the public all have a role to play in achieving this aim. As such, this submission responds to the three topics set out by the CMS Select Committee with a focus on how the internet is used by and could be made safer for children and young people. Most notably, this document includes recommendations for:

AGE-INAPPROPRIATE MATERIAL:

- All Internet Service Providers to create simple ways for all internet customers to regularly make clear and meaningful choices around content controls for internet-enabled devices in the home, and for the effectiveness of these filters to be evaluated frequently.

¹ ChildLine “online issues” statistic 2011/12

- Digital judgement and e-safety to be a component of sex and relationship education that is a compulsory part of the national curriculum.

CHILD ABUSE IMAGES:

- Industry to act swiftly to find and put into implementation a technological solution to block more searches for child abuse images.
- Greater police prioritisation and resources to bring offenders to justice.
- International collaboration in combatting the making, viewing and sharing of abhorrent child abuse images across the internet.

HARMFUL CONTACT ONLINE:

- A dual response from the education system and the internet industry to prevent and respond to harmful online behaviour like cyber bullying and online sexual grooming.

TOPIC ONE: HOW TO BEST PROTECT MINORS FROM ACCESSING ADULT CONTENT

5. The NSPCC would like to encourage the CMS Committee to consider how best to ensure children and young people are accessing content that is appropriate for their developmental age rather than simply looking at this challenge as a binary under 18/over 18 problem.

6. For instance, research the NSPCC is about to launch shows that while many of the biggest social networking sites, such as Facebook, Twitter and YouTube, require users to be over the age of 13 to have a profile, large numbers of children under the age of 13 are active users of these sites and, therefore, potentially exposed to content that is not appropriate for their developmental age.

What we know from ChildLine

7. During 2011–12, there were 641 counselling sessions where the young person specifically mentioned being exposed to sexually indecent images.² While these incidents will not exclusively relate to online content, a large proportion of this sexually explicit material will have been accessed through internet enabled devices. Young people often told ChildLine that they felt guilty and disgusted about what they had seen and were extremely worried about getting into trouble for accessing these sites. ChildLine has also seen a growing trend of young people talking about being addicted to online pornography.

Filters and parental controls

8. In June 2011 the government published the Bailey Review of the Commercialisation and Sexualisation of Childhood. This Review recommended that it should be made easier for parents to block adult and age-restricted material from the internet. In response, the UK's four biggest internet service providers (ISPs) announced a new voluntary code of practice and the adoption of "active choice" systems for new customers which was rolled out in October 2012. The NSPCC was broadly supportive of this initiative, but at the same time felt that this progress did not represent a panacea, especially as the companies' existing customers would not be encouraged to make a choice about filters and parental controls.

9. Following an independent Parliamentary inquiry into "Online Child Protection" led by Claire Perry MP and a Government consultation on parental controls, both in 2012, most recently the Prime Minister came to the NSPCC main London office to announce a package of measures to make the internet safer for children and young people. One key call of the Prime Minister's speech was for Internet Service Providers (ISPs) to ensure that not only new but also existing customers are asked to make a choice about applying content filters, with the "filters on" button pre-checked ("active choice plus") by the end of 2014. The NSPCC welcomes this proposal and that a clear deadline for delivery has been set.

10. The ISPs are expected to report back to the Government at the end of October on progress towards this goal. The NSPCC considers it is important that the major service providers are developing uncomplicated and meaningful mechanisms for ensuring customers are making active and informed choices about the filters they apply in their homes. We are, however, keen to see that after the initial decision is made by the customer about the filter package they want in place, the ISPs will ask them to reconsider their choices on a regular basis and that the effectiveness of the filters is evaluated frequently. We believe this would help to ensure the filters remain relevant for children's digital needs and habits over a sustained period of time. We also want to see a commitment from the smaller ISPs to implementation of similar processes to ensure their customers have access to the same level of meaningful choice

Education

11. We believe building children's e-literacy and digital judgement is essential for helping children and young people to understand the challenges they may face when accessing content that is inappropriate for their developmental age and encourage them to make an active choice about avoiding material that might upset

² Ibid

them. The responsibility for this falls on both parents and the schools. However, the NSPCC understands that not all parents, carers and teachers feel equipped to deliver these messages. As such, we believe there is a role for Government to encourage the delivery of this education by:

- Making e-safety an aspect of sex and relationship education which should be a compulsory part of the national curriculum. Teachers should be given suitable training and teaching aids to deliver these lessons.
- Supporting the launch of a national awareness raising campaign aimed at parents to help them understand the risks the internet poses in relation to their children accessing material online that is inappropriate for their developmental age, and to direct them to information to support them to have conversations with their children about this content.

12. We are disappointed that the Government does not plan to update the sex and relationship guidance for schools, which remains unchanged since 2001. We support the *Daily Telegraph* campaign asking Government to reconsider this position.

TOPIC TWO: FILTERING OUT EXTREMIST MATERIAL, INCLUDING IMAGES OF CHILD ABUSE AND MATERIAL INTENDED TO PROMOTE TERRORISM OR OTHER ACTS OF VIOLENCE

13. The NSPCC would like to challenge the CMS Committee's use of the word "filtering" in the context of tackling the making, sharing and viewing of child abuse images online. Filters are tools which should be applied to manage access to content which is legal but possibly not appropriate for younger audiences, not as mechanisms for hiding content which is wholly illegal and should not exist on the internet. Instead we believe the Committee should be talking about "combatting" and "eradicating" child abuse images from the internet as there should be no place on the web for this abhorrent material.

An overview of child abuse images and prevalence

14. Child abuse images are a visual record of the sexual abuse of a child. They can include pseudo-photographs, animations, drawings, tracings, videos and films which are being streamed live. In the UK images are graded on a 1–5 scale. Level 5 images involve sadism or bestiality, Level 4 will portray a child engaged in penetrative sexual activity and so on to Level 1, where the images will depict erotic posing with no visible sexual activity. Please note that the sentencing council is currently reconsidering the definition of level 3.

15. The number of separate child abuse images in circulation is unknown. In 2010, an NSPCC Freedom of Information request revealed that nearly 26 million child sexual abuse images had been confiscated in the preceding two years from just five of the 43 police forces in England and Wales which were able to check their records. Most forces said it would take too long to interrogate files to see how many pictures of children being sexually abused they had accumulated during investigations. However, estimates of the number of online child abuse images confiscated by police in England and Wales each year in the UK range from 100–360 million.³

16. In the past producers of child abuse images were limited in the extent to which they could obtain and disseminate images. However, advances in technology, including the popularisation of the internet has made child abuse images available to a far greater number of people than ever before. Now, once an image has been uploaded to the internet it may be replicated and downloaded an unlimited number of times. The knowledge that images of abuse cannot ever be fully deleted has a profound effect on the victims involved and this may follow them into their adult lives. Victims may also become aware that the material involved can be used to groom and to abuse other children. Perpetrators of sexual abuse have also been known to use sex abuse images as part of the grooming process, in order to desensitise children and young people to the idea of sexual contact.

A proactive response to the challenge

17. The NSPCC was pleased when, in June 2013, it was announced that for the first time the Internet Watch Foundation (IWF) will be working with Child Exploitation and Online Protection Centre (CEOP) to proactively seek and block online child sexual abuse images. We hope this will help to significantly reduce the number of images available on the web. The commitment shown by the UK's leading internet providers, who donated to the project £1 million of extra funding and a signed a "zero tolerance" pledge to help tackle the creation and distribution of child sexual abuse images, was also welcome.

18. While we are pleased that more resource and capacity is being dedicated to the search and take down of child abuse images, the NSPCC does have concerns that there is currently insufficient police resourcing to proactively identify, arrest and seek prosecution of people who are making, sharing and viewing child abuse images. We believe, however, that there is a unique opportunity with the launch of the National Crime Agency (NCA), within which CEOP will now sit, for the tackling of child abuse images to become a key UK policing priority.

19. The NSPCC understands Her Majesty's Inspectorate of Constabulary (HMIC) intends to conduct a programme of Child Abuse related inspections in 2013–14, the first of which will focus on the police service's

³ NSPCC, https://www.nspcc.org.uk/Inform/research/questions/people_convicted_of_child_abuse_images_2010_wda83579.html

response to child sexual exploitation facilitated or caused by use of the internet. We hope that the inspection will address the capacity of forces to investigate crimes relating to child abuse images. More specifically, it is vital that the NCA and local forces have both the necessary expertise and sufficient resources to find and bring to justice people who make, share or view child abuse images.

Detering potential perpetrators

20. The NSPCC is pleased that the major search engines are implementing “splash pages” warning internet users of the crime they are trying to commit and its implications when they try to view a page already known to the IWF to contain illegal or indecent images. We are also pleased to understand that there is commitment from some part of the “search industry” to also developing advice pages offering people clear routes to legitimate sites on the web when terms are used that could be interpreted as a potential searches for images of child abuse.

21. The Prime Minister’s online safety speech in July also included a challenge to search companies to take one further step and deliver “no returns” in certain instances where searchers are unequivocally looking for child abuse images. The NSPCC fully supports the Prime Minister’s call to action and wants search companies to pledge to deliver swiftly meaningful and effective technological solutions to this challenge at the Autumn summit on online safety the Government has committed to host. We also call on the search companies and Government to agree together a robust monitoring process to scrutinise the efficacy of the solution and an approach to tracking and making public progress achieved through these technical solutions.

22. In addition, we welcome the resource the Government has committed to creating a new National Database of Child Abuse Images to work as a central repository for online child abuse images that have been identified and confiscated. We are keen that the Government now sets out a clear timeline for delivery of the database and make public more information about how it will be used in the fight against child abuse images.

23. Lastly, we ask the Government to explore the potential of creating a public awareness campaign aimed at people who might consider making, viewing or sharing child abuse images informing them on the possible consequences of their actions and directing them to support services, like Stop It Now!

The international dimension

24. The UK Government has shown leadership in the battle against child abuse images. However, the NSPCC, like others, regards the issue to be a global problem. We believe to make significant inroads to tackling the dissemination of child abuse images online, greater international cooperation and activity is required with more countries buying-in to the need for effective search and take down mechanisms. We are pleased that a UK/US taskforce has been established to look at the international dimensions of this challenge and we urge the taskforce to look into the feasibility of:

- The new UK National Database of Child Abuse Images playing a role as part of a bigger global network of image databases and from this network a global process for proactively searching for, reporting and removing child abuse images being established
- Greater prioritisation of technological solutions to disrupt peer-to-peer networks and sharing across the darknet
- Relevant internet companies agreeing to an accord of information sharing in the name of disseminating best practice in the field of search and take down technology

TOPIC THREE: PREVENTING ABUSIVE OR THREATENING COMMENTS ON SOCIAL MEDIA

25. As well as issues around the content that is available on the internet, either inappropriate or illegal, a significant challenge young people face is learning how to behave in a responsible and socially acceptable way while online and knowing how to respond to unwanted contact or engagement via the internet.

26. The main issues about which young people talked to ChildLine counsellors when discussing online safety were cyber-bullying, online sexual abuse, sexting and social networking issues. The NSPCC has found that almost a quarter (23%) of 11 and 12 year olds who have a profile on a social networking site say that they have been upset by something on it over the last year. We respond to this section of the inquiry by focusing on two distinct aspects of abusive and threatening behaviour on social media that affects children and young people: a) peer to peer cyber bullying and b) online sexual grooming. We then explore the policy solutions that could be used to tackle both online dangers.

Cyber bullying—the extent and impact

27. The ChildLine website describes online bullying to young people as: “when a person or a group of people uses the internet, mobile phones, online games or any other kind of digital technology to threaten, tease, upset or humiliate someone else...” The perpetrator can be known to the victim or they can make themselves anonymous by setting up fake accounts or by using public computers so that their own personal IP address can’t be traced.

28. It can happen at all times of the day and inside the young person's home or somewhere they may have previously felt safe. As a result the young person may feel trapped and that they are unable to escape. Traditionally guidance given to young people on how to handle bullying would be "to walk away"; however this advice has now become redundant. In a world dominated with technology a young person is no longer able to walk away from the situation.⁴

29. In 2012–13 Childline saw an 87% increase in counselling session about online bullying. We've also seen from the ChildLine messaging board just how significant an impact this experience can have on young people.

"she gets all her friends against me...every time I look at my messages it's something about the way I look or my personality- swearing at me and telling me to kill myself. I'm tempted to commit suicide". ChildLine message board user

"The lad who bullies me has made a new Facebook account and was spreading rumours about me which everyone believes. Everyone began writing status's about me/calling me 'twisted' 'sick in the head' 'waste of space'. I was even told to kill myself...I'm scared to go to school tomorrow. I've been crying all weekend...I don't know what to do". ChildLine message board user

Online grooming—the extent and impact

30. Grooming can be defined as actions that deliberately establish an emotional connection and trust with a child or young person, with the aim of engaging them in sexual behaviour or exploitation.⁵ Online grooming is exactly the same, but done through the internet, and using technology such as smart phones, laptops, tablets and computer game consoles. The exact numbers of children who are subjected to online grooming is unknown. However, we do know that in 2011–12 The NSPCC's ChildLine service had 413 contacts from children where the primary concern was grooming. Sixty% of these specifically mentioned online grooming.⁶

31. Many young people will not disclose the offences against them online because they feel shame and guilt about the way they have been made to feel, and mistakenly, that they are somehow responsible for their own abuse, for example when they have posted explicit images or had conversations online that can never be erased.⁷ While other victims deny the abuse happened or are unaware that they were being abused, thinking that they were chatting or meeting up with their "boyfriend".

A solution—education

32. As mentioned above, online bullying and online sexual exploitation are very distinct and separate challenges. However, education has a role to play in helping to prevent both problems.

33. In the case of online grooming children and young people need to be taught about how to be resilient—keeping personal information safe, blocking unwanted sexual approaches, talking to a trusted adult about contact they have received online that they are uncomfortable with. While with online bullying, children need to understand more about pro-social and respectful behaviour both in their face-to-face contact with their peers, but also in their virtual interactions.

34. Re-emphasising what we called for previously in this submission, the NSPCC wants to see sex and relationship education being taught as a compulsory part of the national curriculum and for online safety featuring the components listed above to be included as a key part of these lessons.

A solution—monitoring and reporting

35. The NSPCC also believes social networking sites and others who provide online services and products to children have a corporate social responsibility/duty of care for protecting children and young people from harmful contact with both peers and adult sexual predators. More specifically we would like to see:

- Providers should ensure that there are a range of options for how site users report illegal, offensive or abusive content, and these are easy to find and use
- Social networking sites in the UK to provide a simple route for younger users to seek support and help via ChildLine.
- Default privacy settings should be set to the highest levels possible and any avenues for anonymous contact set to "off" for children under 18.

⁴ Digizen (2013) "Understanding Cyberbullying", available from: <http://www.digizen.org/resources/cyberbullying/understanding/how-is.aspx> [Accessed on 27 August 2013]

⁵ Turnbull, M (2012). Caught in a Trap: Impact of Grooming in 2012. London: ChildLine

⁶ Ibid

⁷ Palmer, von Weller and Loof. (2010) The impact of internet abuse on children and how best to intervene; The Link—The Official Newsletter of the International Society for the Prevention of Child Abuse in Neglect (ISPCAN) Colorado USA

- Adequate use of human moderators on social networking sites so that appropriate and timely action can be taken in response to a) breaches in the sites' codes of conduct b) abusive or threatening behaviour c) potential illegal activity.

September 2013

Written evidence submitted by BeatBullying

1. INTRODUCTION TO BEATBULLYING

1.1 BeatBullying is the UK's leading bullying prevention charity, creating a world where bullying, violence and harassment are unacceptable. BeatBullying empowers people to understand, recognise, and say no to bullying and cyberbullying, violence and harassment, by giving them the tools to transform their lives and the lives of their peers.

1.2 As an organisation with children's and young people's safety (both online and offline) at its heart, BeatBullying's online programmes have embedded user protection mechanisms at several levels from the beginning. Users have access to all the functions of a social networking site—email-style private messaging, instant messaging chat in real time, a customisable profile page, the chance to upload content including blogs, and a chatroom—but with the safety and wellbeing of its users built in as a core priority across every aspect. The BeatBullying site is fully moderated for language and content both by software and by human moderators; all content is checked and approved before being uploaded; the site has clearly stated rules for safety and behaviour which users are expected to follow, with a system of sanctions for breaking them; staff and moderators can eject, ban and block any user whose behaviour is unacceptable; there are extensive reporting systems in place both for users to report issues such as bullying by others on the site and for staff to share information, including the reporting of users who appear to be adults. BeatBullying.org is the only e-mentoring and social networking site to be endorsed by CEOP. We strongly believe that our approach to online safety must be adopted by all internet providers if children and young people are to be safe online.

2 SUMMARY

2.1 BeatBullying's online programmes all utilize a combination of approaches to keeping children and young people safe online, of which the technical safeguards outlined above are a fundamental part. However, these cannot be considered in isolation from the other aspects of our work—education, support, attitude and behaviour change, and empowerment—which are just as fundamental.

2.2 BeatBullying is completely in agreement with the principle of preselecting to block genuinely harmful content such as pornography but could not endorse any system that might deny access to legitimate information, advice and support around sensitive issues due to over-zealous and inadequately nuanced filtering.

2.3 The most useful "parental control" is parental responsibility and, inseparable from this, the commitment to developing their children's own sense of responsibility as they grow up.

2.4 Blocks and filters can only block and filter; they cannot educate children about how to deal with the kind of content and behaviour they might encounter online, how to manage their own behaviour responsibly or why certain material is harmful.

2.5 Everyone involved with children's and young people's use of the internet—parents, schools, service providers, organisations and children themselves—has a shared responsibility for online safety. That is why in April 2013 BeatBullying launched a campaign for better anti-bullying protections called Ayden's Law.⁸ The campaign calls for a national strategy to tackle cyberbullying and would set out how the voluntary and community sector, parents and schools would be equipped to (a) protect the children in their care from harm online and (b) educate and equip children about internet safety and responsible digital citizenship so that they understand the issues for themselves.

2.6 Any approach to online safety must ultimately be about shaping attitudes and changing behaviors as much as it is about teaching techniques for staying safe or for anything else.

3 HOW BEST TO PROTECT MINORS FROM ACCESSING ADULT CONTENT

3.1 Findings from our recent survey of children and parents⁹ show that the majority of parents and children (78% and 48%) agree that parents should mainly be responsible for controlling what children access online with two thirds (66%) of parents feeling confident enough to advise their children where to go online.

3.2 Whilst we understand that parents have a responsibility to protect minors from accessing adult content online, we would argue that parental controls are only part of the wider issue of responsibility. The most useful "parental control" is parental responsibility and, inseparable from this, the commitment to developing their children's own sense of responsibility as they grow up. It is imperative that children and young people are

⁸ Launched May 2013 with The Sun Newspaper following the tragic death of Ayden Olsen Aged 14

⁹ The Online Behavioural Habits of Young People Today, which questioned a 1000 8–16-year-olds and 1500 parents from Parentdish and BeatBullying, July 2013

encouraged to take appropriate responsibility for themselves and their own behaviour increasingly, so as they grow up but beginning in small ways at an early age. In this way, while parents and other adults will still be highly involved, children can be supported to grow up with the idea of responsibility as something integral to, rather than entirely outside of, themselves. Our peer mentoring system works on the premise that children and young people can and do rise to the challenge of appropriate responsibility, properly supported at every stage by older peers and trained adults. Of course online safety cannot be the responsibility of children in isolation, but neither can it be the responsibility of parents alone.

3.4 Over half (57%) of the 11–18 year old respondents surveyed in 2012¹⁰ told us their parents talk to them about online safety and what they should or should not look at on the internet as a way to keep them safe online. As the largest category of response this indicates that among our respondents a majority of parents are actively engaged in their children's use of online technology. Over a quarter (27%) say that their parents do not use any methods (technological or otherwise) of keeping them safe online and a fifth (20%) say that they use technological filters. Almost the same proportion (17%) report that their parents encourage them to use websites about internet safety, and 12% say that their parents sit with them while they are online and watch what they do. Further written responses included "offering non-intrusive advice" and "trust", which illustrate an aspect of the online safety debate which is often overlooked: the relationship between parent and child and its bearing on the development of trustworthiness. This reinforces the argument for increased education for children/young people and parents, ideally helping them to develop a continued dialogue about the use of the internet.

3.6 Under 18 is a broad category; while we agree that there is some material that no-one under this age should be able to access, there are also many grey areas: some things that would be completely off-limits to a primary-school child might be fine for a 14 year-old. Just as in the offline world, older teenagers are expected to have much more independence than young children; what would be appropriate for a seven year-old and for a 17 year-old to view or engage with online are going to be very different. CHIS (Children's Charities Coalition on Internet Safety) suggests the possibility of allowing different user accounts to be set up for users of different ages in a single household, via routers that are built for this specific purpose; BeatBullying supports this, with the caveat that age verification systems need to be more advanced in order to ensure that it works as it should.

4 Filtering out extremist material, including images of child abuse and material intended to promote terrorism or other acts of violence

4.1 Leading on from parental responsibility, it is important to recognise that the technical safety features of these sites are integral to the sites themselves. It does not matter where a user accesses them from, on what device, or through which network, the safety features remain consistent.

4.2 BeatBullying is completely in agreement with the principle of blocking genuinely harmful content such as pornography but could not endorse any system that might deny access to legitimate information, advice and support around sensitive issues due to over-zealous and inadequately nuanced filtering. It would be valuable if categories subject to filtering were broken down into more meaningful neutral, positive and negative sub-groups, such as: "Eating disorders—general information" (neutral), "Eating disorders—advice and support for prevention or recovery, such as the charity Beat" (positive) versus "Eating disorders—pro-anorexia (negative)" and parents could make a separate decision in each of these distinct categories.

4.3 BeatBullying is in favour of the Government's "pre-select to on" approach to filtering. This option has the virtue of simplicity for parents, setting up blocks as the default and requiring a conscious and deliberate opt-in for certain content. However, as explained above, we would welcome more detailed scrutiny of what is or is not acceptable: categories such as "violence" or "anorexia/bulimia" in themselves tell us nothing.

4.4 Implicit in having certain things ready-blocked is a "social norm" of what is and is not acceptable. The assumption inherent in pre-blocked content is that parents will not want their children to access pornography etc., and the idea is that this acts as a prompt to conform to this expectation. While we believe that the majority of parents are responsible, there is a minority who might lack either the capacity or the will to make informed decisions in this area. That is why we take the view that having automatic blocks on some content, which can be removed by adults if they choose, would be the best option to ensure a balance between guidance and freedom, thereby protecting children more effectively.

4.5 It is important that in a time where technology has outstripped the capacity of law enforcement, filtering and blocking is not just at the feet of parents; it is imperative that search engines and ISP's actively challenge themselves to work towards an advancing solution to an on-going problem. In July this year the Prime Minister threatened legislation if internet providers failed to commit to a blacklist of CEOP search engine terms which we support and hope that progress is swift.

4.6 Since 2008 the UK Council for Child Internet Safety has tried but failed to introduce meaningful self-regulation. BeatBullying would therefore introduce regulations on internet safety that would:

- Ensure clearer and simpler mechanisms for children to report cyberbullying or abuse.
- Agree protocols in response to reports of cyberbullying or abuse. This includes initial response times and timescales on the removal of harmful content.

¹⁰ Parental Internet Controls Survey: Children and Young People's (2012)

- Ensure robust moderation of user generated content.
- Request prominent signposting to sources of expertise, advice, support and help.
- Require independent monitoring of a code of practice for industry, with results promoted to parents and children.

5. PREVENTING ABUSIVE OR THREATENING COMMENTS ON SOCIAL MEDIA

5.1 Our latest survey¹¹ of children and parents found:

- One in five 12–16 year-olds have interacted with strangers online.
- More than a third of 12–16 year-olds go online most often in their own bedroom.
- One in five 12–16 year-olds think being bullied online is part of life.
- More than a quarter of 12–16 year-olds admitted to witnessing bullying online, but only half did something about it.
- The primary reasons young people gave for not doing anything about the online bullying was being worried about being bullied themselves or not knowing who to speak to about it.
- Almost a quarter (23%) of 12–16 year-olds spend more than five hours a day online during school holidays. More than double the number during term time (10%).
- The majority (80%) of 12–16 year-olds said they feel safe online, compared to only 60% of the younger age group (8–11 year-olds). But worryingly, one in five (22%) of 12–16 year-olds said they think being bullied online is part of life.
- For those 12–16 year-olds who did do something about the cyber bullying, most went to their parents for advice, however only 38% of parents think their children are at risk of being bullied online.

5.2 Whilst there are technological advances that allow streams of text to be analysed and flagged up for bullying behaviour, BeatBullying works to educate and empower children and young people to take responsibility for their actions and understand that bullying in any form is unacceptable.

5.3 Among primary-school children who participated in our 2012 research,¹² 6% of those who had experienced cyberbullying had been targeted on a hate site or hate group (often referred to as Trolling), 9% had had embarrassing images circulated and 10% had had a photo edited to make fun of them. There are also qualitative accounts of children this age experiencing death threats and sexual harassment online. Among 11–16 year-olds who had been cyberbullied, 6% reported receiving a message or image on the subject of sex which had made them feel uncomfortable or upset. Of those who knew who had sent it, the vast majority (80%) said that it had come from someone around the same age.

5.4 This research found that one in 13 secondary-school and one in 10 primary-school-aged children had been subjected to an intensive, relentless campaign or online attack over a period of weeks, months or even years by other children or young people. Many online phenomenon's such as "sexting"—sending sexual pictures and messages via mobile phone—is overwhelmingly peer-to-peer; it is an instance of children and young people victimising each other and unknowingly victimising themselves, by sharing photos that can be used as weapons for bullying or end up in the hands of adult predators. This perfectly illustrates the point that a significant proportion of negative online content is generated by young people themselves. Given this, it is a concern that any discussion of technological blocking and filtering systems in isolation does not take into account the interactive and user-generated nature of some harmful material, which is likely not to come within the scope of a filter anyway. To our knowledge, it is not possible completely to block interactions such as bullying or "sexting", although, as outlined above, there are both technological and human ways of curtailing these and limiting the harm done. Blocks and filters can only block and filter; they cannot educate children about how to deal with the kind of content and behaviour they might encounter online, how to manage their own behaviour responsibly or why certain material is harmful.

5.5 That is why BeatBullying has been calling for several years for education programmes focusing on behaviour and addressing issues such as cyberbullying and e-safety, to be introduced into all schools. We support and welcome the proposed changes on e-safety to be introduced in the 2014 national curriculum across all key stages. It is clear that education for safety and good behaviour online needs to begin as early as possible, before cyberbullying even becomes an issue.

5.6 Everyone involved with children's and young people's use of the internet—parents, schools, service providers, organisations and children themselves—needs to be seen as sharing responsibility for online safety. In April 2013 BeatBullying launched a campaign for better anti-bullying protections called Ayden's Law.¹³ This campaign called on the Government to produce a national anti-bullying/cyber bullying strategy which would, for the first time, set out the role of teachers, parents, local authorities, the public, the voluntary & community sector and children and young people themselves in preventing and intervening when bullying and

¹¹ The Online Behavioural Habits of Young People Today, which questioned a 1000 8–16-year-olds and 1500 parents from Parentdish and BeatBullying, July 2013

¹² Virtual Violence II Part II: (2012) BeatBullying

¹³ Launched May 2013 with The Sun Newspaper following the tragic death of Ayden Olsen Aged 14

cyber-bullying takes place. Without the introduction of this strategy, progress in tackling online bullying and other safety threats will always be frustrated by the lack of understanding of roles and responsibilities by those charged with keeping children safe online.

5.7 A national strategy to tackle cyber-bullying would set out how the voluntary and community sector, parents, schools, LAs and the police would be equipped to (a) protect the children in their care from harm online and (b) educate and equip children about internet safety and responsible digital citizenship so that they understand the issues for themselves. The implementation of this can be greatly facilitated by a solid technical framework of support from business, such as Claire Perry's work with internet providers to introduce preselected parental controls or the adoption of the measures listed in para 4.6 above.

5.8 More than 1,700 cases involving abusive messages sent online or via text message reached English and Welsh courts in 2012. However, cyberbullying is not a specific criminal offence in the UK. Some types of harassing or threatening behaviour—or communications—could be a criminal offence. These laws were introduced many years before Twitter, Facebook and Ask.FM, and they have failed to keep pace with the demands of modern technology. Unfortunately, serious cases of cyberbullying, which have often resulted in suicide, have dominated our headlines in recent months. That is why BeatBullying have been calling on the Government to review current legislation and make bullying and cyberbullying a criminal offence so that children and young people have the protection they need and deserve, at the earliest opportunity, to avoid this escalation. This year we have worked with Tracey Crouch MP to introduce bullying and cyberbullying as a form of anti-social behaviour, which will result in victims and perpetrators benefiting from earlier interventions and support outlined in the current Anti-Social Behaviour, Crime and Policing Act Bill.

5.9 For BeatBullying, the approach to online safety must ultimately be about shaping attitudes and changing behaviors as much as it is about teaching techniques for staying safe or for anything else; it is about equipping young people with the inner resources that will keep them safe, and responsible, long-term. Some negative online behaviors such as cyberbullying and sexting are most likely to be a form of child-on-child aggression rather than adult-generated; in order to tackle this successfully, it is crucial to work with perpetrators as well as victims to address the attitudes that underlie the behaviour.

September 2013

Written evidence submitted by the Internet Watch Foundation

- “Online Safety” is a very broad concept that covers a wide and diverse range of issues. When addressing this topic, it is important to clearly identify the issue at stake as different problems will require different solutions, from a technical as well as a procedural perspective.
- The Internet Watch Foundation is concerned that the issues relating to legal adult content filtering and the fight against criminal child sexual abuse images become conflated.
- The Internet Watch Foundation has been very successful in fighting child sexual abuse images and videos on the internet and has become one of the most successful hotlines in the world.
- The success of the Internet Watch Foundation is mainly due to its specific focus on child sexual abuse content and the continuing support from the online industry.

THE IMPORTANCE OF CLEARLY DEFINING THE PROBLEM

1. Different problems require different solutions and it is therefore important to clearly distinguish between the different issues under consideration. Combatting illegal online content (which is content that by definition should not be uploaded or viewed by anybody) is different from protecting minors from accessing harmful content (for instance adult content), which is content that in itself is not necessarily illegal. Preventing abusive or threatening comments on social media might be considered a problem related more to conduct rather than content, notwithstanding that the result of this conduct leads to abusive or threatening online content (ie the actual comments).

2. The merit of taking into account the various aspects of online safety lies in the fact that each of these specific issues opens up a different range of possible solutions, both on a technical as well as a procedural level. Other actors can be involved, other safeguards and processes developed. The most effective solution in one area of online safety could therefore be very different from the preferred solution in another. Equally, an effective solution in one area might have negative implications for the effectiveness in another area. Considering the various different challenges individually will protect against developing general, however well-intentioned, solutions that might have an unforeseen negative impact in particular areas of online safety.

COMBATING ILLEGAL CONTENT ON THE INTERNET

3. Even in the area of combating illegal online content, it is important to keep in mind the differences between various types of illegal content, for instance the difference between child sexual abuse content and material intended to promote terrorism or violence.

4. For different types of illegal content different questions have to be considered and depending on the answers different solutions can be formulated. Issues to consider include:

- (i) “What is the nature of the content?” (What is the “level” of illegality? What is the impact on the people viewing the content? What is the impact on the victims of the original crime?);
- (ii) “How is the content available on the internet?” (Where can this content be found? Where is the content hosted? What is the pervasiveness of the content on the internet? How easy is it to find/stumble upon the content?);
- (iii) “What is the preferred solution?” (How important is it to make the content unavailable as quickly as possible? How can this content be found and identified? Who can decide whether the content is potentially illegal? Which involvement of law enforcement/the judiciary is needed at each stage of the solution—identification, investigation, removal?).

5. The answers to these questions will be different when considering material intended to promote terrorism, material constituting a copyright infringement or child sexual abuse material. Depending on the answers, different solutions will be available to effectively deal with the issue and different procedures, actors and safeguards might have to be considered.

FIGHTING ONLINE CHILD SEXUAL ABUSE CONTENT—THE INTERNET WATCH FOUNDATION

6. The UK has currently one of the most effective systems in the world for dealing with child sexual abuse content on the Internet. This success is based on the efficiency and experience of the Internet Watch Foundation (IWF), the support it receives from the online industry and its close cooperation with law enforcement, in particular with CEOP, the UK’s Child Exploitation and Online Protection Centre.

7. *IWF Background:* The IWF is the UK hotline where the public can report child sexual abuse content, criminally obscene adult content and non-photographic images of child sexual abuse. The IWF is a charity founded in 1996 by the UK Internet industry and it is therefore independent from Government and Law Enforcement. However, the IWF has very close working relationships with law enforcement and its operations are covered by a Memorandum of Understanding with the Crown Prosecution Service and the Association of Chief Police Officers and a Service Level Agreement with the Association of Chief Police Officers.

8. The IWF is a membership organisation and is funded by over 100 global members, including internet service providers (ISPs), mobile operators, content providers, hosting providers, filtering companies, search providers, trade associations and the financial sector, as well as by the EU as part of the *UK Safer Internet Centre* together with Childnet International and South West Grid for Learning. As an independent body, transparency and accountability is of the utmost importance and the IWF is governed by an independent Board and the Hotline is independently audited by a highly qualified team every two years. The IWF also operates a thorough complaints procedure and has commissioned an independent Human Rights Review.

9. *IWF processes:* When the IWF receives a report from the public, its analysts assess the content to confirm whether it is within its remit and potentially in breach of UK legislation. If the content is considered to be potentially criminal, the IWF can take action against the child sexual abuse images and videos hosted anywhere in the world. It can also act against criminally obscene adult content and non-photographic child sexual abuse content hosted in the UK.

10. Depending on where the content is hosted, the process for dealing with potentially criminal images and videos differs. When child sexual abuse content is found to be hosted in the UK, the IWF will inform CEOP. After confirmation from CEOP that action can be taken, the IWF will notify the hosting provider who will remove the content from its servers, typically within 60 minutes after receiving the notification from the IWF. This process is commonly referred to as “Notice and Takedown”.

11. When child sexual abuse content is found to be hosted outside the UK, the IWF will inform its counterpart hotline in the hosting country through INHOPE, the international association of hotlines or link in directly with local law enforcement. As other countries take significantly longer to remove child sexual abuse content—50% of the content the IWF passes on internationally is still available after 10 days—the IWF adds the links (URLs) to the content to its URL list (or “blocking list”). IWF members can use this list to voluntarily block access to these URLs to protect their customers from stumbling upon the images and videos. The URLs on the list are as targeted as possible, often comprising a single image or video. This is done in order to prevent the blocking of anything outside the criminal images or videos.

12. In addition to “Notice and Takedown” and the URL list, the IWF also compiles a keyword list of terms that specifically refer to child sexual abuse content. This list is used, for instance, by search engines to prevent people from finding images and videos of child sexual abuse content. The keywords are very specific—or very specific combinations of words—that carry no meaning besides the specific reference to child sexual abuse content. This means the keywords will not prevent access to legitimate websites such as, academic research papers into the area of child sexual abuse or websites aimed to help or inform people in relation to child sexual abuse.

13. Finally, the IWF also monitors newsgroups and can issue notices for removal of individual postings where child sexual abuse content is identified or entire newsgroups if these are being used to specifically distribute child sexual abuse content.

14. *IWF achievements:* In 2012, the IWF processed 39,211 reports and assisted with the removal of 9,696 URLs containing potentially criminal child sexual abuse content. A URL can be as specific as a single image or could refer to an entire website containing potentially thousands of child sexual abuse images or videos. The majority of victims (81%) appeared to be 10 years old or younger (with 4% 2 years old or under) and 53% of the images and videos depicted sexual activity between adults and children, including rape and sexual torture. Over the past 17 years, the IWF has assessed over 400,000 webpages and assisted with the removal of 100,000 URLs containing potential child sexual abuse content. By sharing intelligence with the police, the IWF aided with the identification and rescue of 12 children in the past three years.

15. *IWF success:* In the past decade, the UK has become the world leader for dealing with child sexual abuse content and the IWF is considered as one of the most successful hotlines in the world. Both the amount of reports received/processed by the IWF and the speed with which action is taken is amongst the best within Europe and beyond. As a result, the share of child sexual abuse content that is hosted in the UK is less than 1% of the total amount of known content, down from 18% in 1996 when the IWF first started. This means that—because of the efficiency of the current system—the UK has become an extremely hostile territory to host child sexual abuse content.

16. The success of the IWF is foremost due to its very clear and specific remit. Because of the strong focus on child sexual abuse content, the IWF has accumulated a very thorough and extensive knowledge on how to deal with this content effectively. On the one hand, this means the IWF's analysts have become experts in this area, often recognising images and even victims/perpetrators within the images. They can pass on this information to law enforcement to aid the investigation into the sexual abuse. On the other hand, the IWF has been able to develop a strong network to fight the availability of child sexual abuse content. This multi-stakeholder approach is crucial for successfully dealing with child sexual abuse content and the IWF has built a very strong network, both with law enforcement, the online industry and international partners, for specifically dealing with child sexual abuse images. In addition, the success of the IWF is also a result of its self-regulatory model which allows the IWF to adapt quickly to new developments and of the strong support it has received from the online industry over the past 17 years.

17. *IWF future:* The online environment is ever changing and the IWF is committed to continue developing in order to fight child sexual abuse content effectively in the future. Following a donation from Google and additional funding from other Members, the IWF will increase its number of analysts from 4.5 (full-time equivalents) to 11.5 (full-time equivalents). In addition, the IWF was asked by Government to start proactively searching for child sexual abuse content rather than working only from public leads. The IWF will continue its role as the UK hotline but will be able to add-on the proactive work in order to increase the amount of child sexual abuse images it can take action on. An ongoing membership review is addressing the need to improve IWF's resources in order to ensure a sustainable future for the IWF and its increased activities.

18. A final aspect of IWF's future development concerns its international activities. As 99% of the known child sexual abuse content is hosted abroad, it is of the utmost importance that international cooperation is further developed to remove the child sexual abuse images and videos at source. The IWF is actively engaging with international partners to share its expertise. It has developed "OCSARP", its "Online Child Sexual Abuse Reporting Portal", which countries without child sexual abuse content reporting facilities can implement, while the IWF provides assistance with the assessments of the reports.

CONCLUSION

19. The area of "Online Safety" is very broad and very volatile, with risks as well as possible solutions developing constantly. It would be worthwhile to clearly frame the debate and break up the overall topic in clearly defined aspects of online safety. Online conduct is different from online content. Criminal or illegal content is different from legal but potentially harmful content and an image of a child being sexually abused is different from the promotion of terrorism. This is not to say there is necessarily a hierarchy between the "severeness" of different types of illegal content, but different types of content will require different procedures, different checks and balances and the involvement of different actors.

20. The IWF—and the online industry—has been very effective in fighting child sexual abuse content over the past 17 years. The IWF's very specific self-regulatory and multi-stakeholder model is extremely effective for dealing with child sexual abuse content and the IWF remains committed as ever to continue developing and improving the fight against child sexual abuse content in the years to come.

Written evidence submitted by Internet Services Providers' Association (ISPA)

INTRODUCTION

The Internet Services Providers' Association is the trade association for the internet industry in the UK. ISPA has over 200 members from across the sector, including a large number of access provider ISPs from small to large, content platforms, hosting providers and others. ISPA therefore works across the areas in which the Committee is looking and we welcome the opportunity to provide input into the Committee's inquiry.

We believe that the Committee's terms of reference for the inquiry identify the key issues that are currently of relevance in relation to online safety. However, we would like to emphasise that the issues that have been identified should not be conflated. The issue of tackling child abuse content, which is clearly illegal, requires a different response from industry and Government than the availability of extremist material which may or may not be illegal. Protecting children from accessing potentially harmful content again requires a different response as it may cover content that is clearly legal but simply not appropriate for children and young people under 18.

We further welcome that the Committee considers that any potential dangers of the internet are a "correlation of the immense benefits provided by unimpeded communication and free speech" and that "any attempts to mitigate harms have to be proportionate and, where possible, avoid disadvantageous consequences." We believe that the recognition of this correlation is of vital importance but are concerned that policy-makers sometimes disregard it which often leads to disconnected and potentially harmful policy-making.

VARIETY OF INTERNET COMPANIES

It is important that the Committee understands that there is a considerable diversity of companies that operate internet services. When considering the steps that industry can take, it is important to consider that each type of company may be playing a different role, and they will have varying degrees of ability to deal with potentially illegal or harmful content. The below description provides a rough guide¹⁴ to the various kinds of companies that are involved in making the Internet work. If it were felt to be helpful, we would be happy to brief the Committee in more detail about the position of each company type in the internet value chain.

ACCESS PROVIDERS

Access providers are commonly referred to as Internet Service Providers. They connect customers to the Internet—either through fixed or wireless connectivity. As the ISP does not initiate or modify their users' communications and is only passing traffic across a network, they are deemed "mere conduits" under the E-Commerce Regulation 17 which grants limited liability.

HOSTING PROVIDERS

Hosting providers store others' content online, often for a charge. Traditionally hosting providers have hosted complete websites of individuals and companies and even Government hosts some of its websites with these private hosting providers.

More recently, new types of hosting provider have emerged. These providers, eg social networks, generally provide a platform on which users can upload content (videos, blog posts, images etc.) which they themselves have created. These kinds of hosting provider do not have editorial control over what is posted on their services, but may have active or passive moderating policies that allow them to remove content or restrict its availability.

Under Regulation 19 of the e-Commerce Regulations both traditional and modern hosting providers are not considered to be liable for the content they host as long as they do not have actual knowledge of unlawful activity or information. However, upon obtaining such knowledge, hosting providers become liable if they do not act expeditiously to remove or to disable access to the information.

WEBSITES WHERE OPERATORS HAVE EDITORIAL CONTROL

Individuals, companies and other organisations that run their own websites can be regarded as having editorial control over content that is available via their website and so are considered to have more direct responsibility. However, it is important to point out that websites can contain both content where the operator of a website has editorial control, eg a news article, and user generated content, eg comments about that news article.

SEARCH ENGINES

Search engines index web pages by scanning the Internet. They use algorithms to display relevant results based on what search terms users input but generally do not exercise editorial control over the links that they present to users. Search engines can be considered as "caches" under Regulation 18 of the e-Commerce

¹⁴ We merely consider the e-Commerce Regulations and online companies may have duties and defences through other legislation.

Regulations and act expeditiously to remove or to disable access to any information if they are made aware of that the fact that this information may be illegal.¹⁵

How does this apply in the real world?

It is worth considering three different examples:

1. A website hosting child abuse images
2. A person who posts a potentially illegal message on a website operated by the same person
3. A person who posts a potentially illegal message on a forum operated by a third party

In relation to the first example, ideally the hosting providers who provides the space for the website should be notified that illegal material is being hosted on a website on one of its servers. This notification is being done on a regular and effective basis by the IWF. If the operator is based outside of the UK and responds slowly or not at all to a notice from the IWF or its international partners, the IWF can add this page to its list of illegal websites. Access providers accept the judgment of the IWF, which has great expertise in this area, and use the IWF's list to filter out the relevant page (ie they make the URL of that website inaccessible, and a user would see an error message if they attempted to access it).

In relation to the second, the person should be approached directly as they have editorial control of the comment and the website on which it can be found. If the person does not respond then it may be necessary to contact the hosting provider who provides the space for the website who may then need to make an expeditious assessment of the content and take it down if appropriate. The access provider would theoretically be able to block access to the website but this would be less timely and cost efficient than approaching the hosting provider and generally requires a valid takedown notice.

In relation to the final example, again, the person who posted the content should be approached directly. However, if the person does not respond, or cannot be identified, the third party who operates the forum should be approached who will then need to make an expeditious assessment of the content and take it down if appropriate. If the third party does not react then it may be necessary to approach the hosting provider, however, this should be a matter of last resort as the provider would generally only be able to remove the whole forum, thereby curtailing the service and rights other forum users. The same would be true if an access provider would block access to the forum.

In all these examples it is important to note that it is often not clear cut whether content is illegal or not and online companies cannot be expected to be the judge and jury of others' content.

INDUSTRY HAS A ROLE TO PLAY

We strongly believe that the industry has a vital role to play in protecting minors from accessing inappropriate content and would like to emphasise that the UK is widely regarded as having one of the most advanced online safety frameworks.

FAMILY FRIENDLY FILTERS

- The main consumer facing ISPs are moving to system where new and existing customers are presented 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, put users in control and allow parents to choose from a list of content that should be filtered including adult content, extremism and self-harm. This has involved significant investment, both financially and time.
- Some smaller consumer-facing providers are considering solutions that offer family friendly filters but can be deployed on smaller scale and at lower costs. ISPA is currently discussing this issue with its members.

CHILD SEXUAL ABUSE CONTENT

- ISPA and many ISPs have helped to setup the IWF and have consistently supported the organisation which is considered to be world class in preventing people from access child abuse content and facilitating the removal of that content at source.
- Many ISPs have committed to increase funding of the IWF to enable a proactive remit to identify and remove child abuse content online. Further funding for education and awareness campaigns from industry has been forthcoming.

¹⁵ Regulation 18 defines providers as "caches" if the information that is processed by them is "the subject of automatic, intermediate and temporary storage where that storage is for the sole purpose of making more efficient onward transmission of the information to other recipients of the service upon their request", ie, the provider merely processes information and only stores it temporarily.

ALLEGEDLY/POTENTIALLY ILLEGAL CONTENT

- Industry has worked with the Home Office and law enforcement regarding the Counter-Terrorism Internet Referral Unit (CTIRU) which members of the public can report potentially unlawful terrorist material from the internet. If hosted in the UK the content is removed and this framework is underpinned by the Terrorism Act 2006. So far approximately 6,500 pieces of online content have been removed through CTIRU action.¹⁶ However, what constitutes terrorist material is not always clear cut.
- Providers of social media platforms and websites that contain user generated content will remove illegal content whenever they are made aware of it and can apply their terms and conditions to other types of content that may not be illegal. They also often provide their consumer with report facilities to flag up any inappropriate behaviour.
- Providers have been working alongside Government and Parliament to reform the defamation law to ensure that online freedom of speech is adequately balanced with the right of those who feel they have been defamed online.

INDUSTRY CANNOT SOLVE THESE ISSUES ON ITS OWN

However, we are concerned that the current policy debate is sometime too strongly focused on finding a technological fix to a problem that often has societal roots and is sometimes present in both the offline and online world.

For example, in the relation to the accessibility of adult content, we accept that ISPs should play a role in empowering their customers to better determine what content should be available in their household. However, even the most comprehensive filtering solution cannot guarantee that adult content will be unavailable. Over and underblocking of content is inevitable and it is important that filtering tools are viewed as part of a wider package alongside education and parental mediation. There needs to be more emphasis on enabling parents and teachers to teach children how to behave responsibly online, one possible action could be the updating of sex education in the curriculum so that it keeps pace with technological and societal developments.

In relation to abusive or threatening comments online, we would like to emphasise that ISPs should not be used as proxy for enforcing the law and perceived societal standards. Social media networks can and often take action against users that behave inappropriately. However it has to be taken into account that the Crown Prosecution Service's Guidelines on prosecuting cases involving communications sent via social media state that "[j]ust because the content expressed in the communication is in bad taste, controversial or unpopular, and may cause offence to individuals or a specific community, this is not in itself sufficient reason to engage the criminal law." This should not be regarded as a get out clause for providers but it is important to point out that providers cannot be expected to go beyond what is required by the law. In this context, it worth highlighting that Parliament has recently amended the Defamation Act which encourages hosting providers to assist the resolution of disputes between users that cannot be resolved by the hosting provider themselves

CONCLUSION

We have shown that industry has made available a number of tools, services and advice to help protect minors from accessing adult content. There is cooperation between industry and law enforcement to tackle extremist material when legal thresholds are crossed. Websites have in place mechanisms to prevent abusive behaviour and the law had been used to prosecute individuals in some instances.

The Internet has had a significant impact on modern societies. It has changed how we do business, communicate, educate and consume content. These changes came about because internet companies developed innovative products and consumers have found even more innovative and sometime unexpected ways of using these products. As such the Internet is an extension of the established offline world and it would be wrong to simply ask ISPs to fix any issues that may arise.

Technological fixes can play a role and support customers but we will only be able to comprehensively tackle the problems that the Committee outlined in its terms of reference by involving industry, Government, parents and users and by looking at both the symptoms and causes. The Internet industry has reviewed and improved its offering to customers in recent times. It is willing to actively engage with the online safety agenda but we hope that this can be done in a more positive environment based on collaboration.

October 2013

¹⁶ HL Deb, 23 September 2013, c421W.

Written evidence submitted by TalkTalk

SUMMARY

1.1 As the first internet company to introduce a whole home parental control solution, TalkTalk welcomes the Committee's Inquiry into Online Safety. We firmly believe that everyone should be able to enjoy the benefits of the internet, but that as an ISP we have a duty to provide our customers with simple and effective tools to ensure that they are able to search, download and utilise the internet in as safe a way as possible, especially when it comes to parents wanting to help protect their children online.

1.2 TalkTalk is currently the only ISP in the UK to offer a whole home parental controls system that protects every device connected to the home broadband. Built into the broadband network itself, HomeSafe gives families the ability to control the types of websites they want their household to access across all devices using the connection and restrict access to content like pornography, gambling, and suicide and self-harm. So far over 1.2 million homes are using HomeSafe, and of these 400,000 have chosen to activate parental controls. In March 2012, we launched so called active or unavoidable choice for all new customers signing up to broadband and in June of this year, we extended this to existing customers and began the process of asking all our existing customers to make a choice about using parental controls.

1.3 1 in 3 customers—roughly equivalent to the number of UK homes with children in—are choosing to use filtering when presented with a choice. Whilst much of the debate on internet safety has focused on children accessing pornography, suicide and self-harm remains the biggest category that customers are choosing to block, followed by pornography which is then followed narrowly by weapons and violence. This reflects the range of concerns that parents have when it comes to their child's safety online and indeed many of their concerns aren't about accessing inappropriate content, but are behavioral such as cyber bullying, sexting and grooming.

1.4 When it comes to filtering, our research shows our customers like being asked to make a choice—80% think it's a good thing and 60% wouldn't have activated controls if they hadn't been prompted. We support this approach and believe that it is critical that parents make an engaged decision, appropriate to their individual family, about the use of filtering tools. We would never filter access to content that is legal (even if it is age-restricted) unless our customers asked us to. Parents should make the decision as part of their approach to helping keep their children safer online.

1.5 As a member of the IWF, TalkTalk does take the IWF list and voluntarily block this at network level so none of our customers can access websites that they have identified to contain illegal child abuse images. In the summer, we—and other ISPS—also implemented a new form of wording on the block pages to act as a stronger deterrent. We are also big supporters of the IWF's move to proactive detection.

1.6 There is no silver bullet when it comes to internet safety, and much relies on education and awareness. TalkTalk conducts extensive marketing and communications to customers about HomeSafe and internet safety and we have also partnered with the likes of the The Parent Zone, Girl Guiding UK and the UK Safer Internet Centre on various educational initiatives. Along with other ISPs, we have committed to launch of a national, sustainable education campaign targeted at parents in the New Year.

1.7 We have long called for internet safety to be included in the Primary curriculum and we are really pleased that will be the case going forward. We think of internet safety as the road safety of our children's generation, in that it required a range of different inventions including the Green Cross Code, air bags and mandatory seat belt wearing, and required us all to play our part. Internet safety requires the same approach where use of technical tools needs to be supported by awareness raising and education for parents and young people alike.

2. HOW BEST TO PROTECT MINORS FROM ACCESSING ADULT CONTENT

2.1. TalkTalk shares the commonly held belief in the importance of protecting children online. The internet is an integral part of people's lives now and has been transformational in terms of the benefits that it brings. However, as with life offline, there are unfortunately risks associated especially for children and young people and we believe we have a role to play in trying to protect them from harm.

2.2. TalkTalk thinks of internet safety as the road safety of our children's generation; it requires a range of different inventions, and the use of technical tools needs to be supported by awareness raising and education for parents and young people alike. We think technical tools have a really important role to play, but alone they will not solve the issue. We believe the most important thing a parent can do is take an active role and talk to their children about what they do online, and combine this with using controls as appropriate.

HomeSafe

2.3 Back in May 2011, TalkTalk introduced HomeSafe, the UK's first and still only whole home parental controls system that allows parents to protect every device connected to the home broadband and control the types of websites their family is able to visit. From our own customer research we found that parents want an easy to use system that allows them to activate their chosen filters across all devices with one click without

having to do this separately on each device in the home. We also found that many parents found existing device level controls confusing and we developed HomeSafe to fill that gap.

2.4 HomeSafe has three simple features; Kids Safe, Virus Alerts and Homework Time.

- *Kids Safe*—parental controls that allow the account holder to block content they don't want to be accessed on their connection. There are nine different categories, and customers can also choose to block other specific websites.
- *Virus Alerts*—an alert system that blocks access to web pages infected with malware and phishing sites.
- *Homework Time*—this allows parents to block social networking and online gaming sites—common sources of distraction for children from homework—during a specified time of day.

2.5 The most commonly blocked categories are, in order, Suicide & Self-Harm; Pornography; Violence & Weapons; Dating; Drugs, Tobacco and Alcohol; Gambling; File-sharing; Gaming Websites; and Social Networking.

Asking our customers to make a choice

2.6 In March 2012, TalkTalk became the first internet service provider to introduce a genuine unavoidable choice for new customers when they signed up to TalkTalk broadband, as per the recommendation of the Bailey Review. Customers are asked to make a “yes” or “no” decision as to whether they want to filter access to content that might be inappropriate for under 18s on their broadband connection or not. TalkTalk then applies this to their internet connection as soon as its live and no further action is required by the customer. If the customer wants this on, then Suicide and Self Harm; Pornography; Weapons and Violence; Dating; Drugs, Alcohol and Tobacco; and Gambling will be blocked. The settings can be easily changed at anytime through the customer's online My Account facility.

2.7 At the beginning of June of this year we extended this unavoidable choice to existing customers and began the process of asking all of our existing customers who haven't yet engaged to make a choice about using Kids Safe filtering. We are doing this via the use of a pop-up screen when a customer who isn't using parental controls logs into their My Account. As with new customers, they have to make a decision either way before they progress any further and access their My Account. We have already asked a million of our existing customers to decide about using Kids Safe.

2.8 We currently have 1.2 million customers who have activated HomeSafe and over 400,000 customers have activated Kids Safe filtering. 1 in 3 customers are choosing to turn on Kids Safe when presented with an unavoidable choice. This is about equivalent to the number of households with children in and so we believe represents the level of uptake that one should expect, given that not all parents will want to use filtering but other customers, like grandparents or those who simply want to filter content out due to personal beliefs, might want to.

2.9 By the end of 2013 we will move to pre-ticking the “yes” option, which we believe is a strengthening of our current position. It is incredibly important however to note that this does not constitute default blocking and all customers will still be asked to make a decision about filtering; we would not filter without them requesting it. We think it is critical that parents make an engaged, informed choice about whether or not they wish to use filtering as part of their approach to helping keep their children safer online.

2.10 Our customers agree with this and our research shows they like being asked to make a choice. A survey of our customers found:

- Around 80% felt that being prompted to set up parental controls was a good thing.
- 60% of those who set up controls said they wouldn't have done it if they hadn't been prompted.
- Of those who didn't activate parental controls 60% said they didn't turn them on because they didn't have children and 30% said they didn't want/need them.

Closed feedback loop

2.11 There are a number of safeguards in place to help ensure that children aren't changing the settings without their parents' knowledge. Firstly, the initial set up is done during the sign up process for fixed line broadband where a customer will likely be credit checked, have to provide bank details and be arranging for a new broadband service to be installed/an existing service to be taken out. They are also entering into a 12 or 18 month contract and our terms and conditions state our customers must be aged 18 or over. Secondly, the log in details for a customer's My Account—where they make any subsequent changes to their HomeSafe settings—are set up during the joining process by the account holder. At any time, from anywhere, the account holder can log in to My Account to check the status of their home's filtering preferences. Every time a change is made to the settings an email is sent to the email address the account holder signed up with confirming the changes. Finally, every customer can also opt in for free additional notifications via SMS to their mobile.

Over-blocking

2.12 We know that there are concerns about over-blocking of websites in relation to whole home filtering systems. Firstly we think it is really important to remember that filtering systems have been in place for years—they were just applied at the device level rather than at the network level. When it then comes to issues around inaccurate blocking, we think there are two key things; firstly obviously that the filtering technology itself is being constantly improved and refined, and secondly that there are clear reporting mechanisms which are actioned.

2.13 In developing HomeSafe we deliberately tried to take a more holistic approach to website categorisation which looks at the website in its entirety—so for example an article on the BBC website which mentions pornography wouldn't be blocked. Similarly, a website like Frank which offers advice for those suffering from drug addiction wouldn't be blocked, whereas a website advising on how to make drugs would be. We think this is a more pragmatic approach. Clearly no technology is 100% perfect and so we continue to work to improve the filtering. We have clear reporting mechanisms, either directly via a large "report" button on the block page itself or through a feedback form in the customer's My Account. Website owners can also contact us via email. This enables us to address any issues of misclassification and also employ any learning to avoid other instances. The volume of this is respectively low and we aim to action reports within five days.

2.14 We have also formed partnerships with a number of companies to either "white" or "black" list. Papyrus, the suicide prevention charity, provides us with a list of websites that promote suicide and we include those in the suicide and self-harm category. Similarly, we have an agreement with the British Association for Shooting and Conservation (BASC) to ensure that websites with content about lawful shooting interests aren't blocked.

Marketing, advice and guidance

2.15 HomeSafe is actively supported by comprehensive marketing and communications that aim to educate our customers about internet safety and the things they can do to help protect themselves and their children online. We have a dedicated internet safety hub (talktalk.co.uk/security) that provides a wealth of guidance. This is currently being updated, including aligning with the UKCCIS guide on child internet safety—which we helped to develop. We also send regular communications about HomeSafe and internet safety to our customers. Other marketing has included extensive television and outdoor advertising; we believe TalkTalk is the only company to have advertised about child internet safety on television. We have also run dedicated security workshops for our customers in London and the key insights and advice from the day are then shared back to the rest of our customer base. For Safer Internet Day this year we ran an internet safety road show which visited 5 locations around the country and offered advice and guidance on internet safety to the public.

2.16 In addition to the above, we run or are involved in a number of additional initiatives to educate and raise awareness about internet safety. We have been working with The Parent Zone to develop 'The HomeSafe Family Challenge', a three-term programme of activity for schools to help them engage parents on child internet safety. Each term covers a specific theme—Digital Footprint, Digital Know How and Digital Living—and within each theme there are a range of topics covered for parents and teachers. The HomeSafe Family Challenge is designed to get parents to engage with the issue and take action. Each theme will have a challenge associated with it to engage parents and encourage action, for example getting a certain number of parents to take the "HomeSafe family challenge quiz" with a prize for the school if they do. We have been trialing this with a number of schools and are now rolling this out to more schools across the UK.

2.17 We have also partnered with Girl Guiding UK to help them redevelop their Computer badge for Brownies and as part of this will produce supporting educational materials on internet safety for both the Brownies and their volunteers as internet safety forms one of the elements of getting the Computer badge. This will be supported by a significant communications campaign about internet safety to the Brownies and their volunteers.

2.18 We have also worked with The Parent Zone to develop a very simple guide to parental controls which has been sent to schools across the UK and is available for free download from their website, and also with the UK Safer Internet Centre to create and promote a video on setting up HomeSafe.

2.19 Finally, along with the other ISPs, we have committed to launch of a national, sustainable education campaign targeted at parents in the New Year.

3. Filtering out extremist material, including images of child abuse and material intended to promote terrorism or other acts of violence;

3.1 Like other industry members, TalkTalk takes a zero tolerance approach to illegal child abuse images online. Currently our efforts are focused on helping prevention. We are a longstanding member of the Internet Watch Foundation and pay the maximum membership fee. This summer we, along with the other ISPs, committed to a further £1 million of funding for the IWF to continue its work in identifying illegal child abuse images on the internet. TalkTalk also chaired the working group that supported the membership review of the IWF which has led to their move to proactively seeking out illegal child abuse images online in addition to following public reports.

3.2 We automatically download the block list of known websites containing illegal images from the IWF on a daily basis, and apply it to our filtering system, which means that every customer is blocked from accessing those websites across the whole network.

3.3 Customers who try and access these websites are presented with a splash page informing them the content is blocked because it has been found to be illegal by the IWF. In the summer, a group comprising the IWF, CEOP and Lucy Faithful Foundation, a charity who work with offenders, agreed a new stronger set of wording that TalkTalk implemented in August, along with the other three major ISPs. The wording is:

Access has been denied by your internet access provider because this page may contain indecent images of children as identified by the Internet Watch Foundation.

Deliberate attempts to access this or related material may result in you committing a criminal offence.

The consequences of deliberately accessing such material are likely to be serious. People arrested risk losing their family and friends, access to children (including their own) and their jobs.

Stop it Now! can provide confidential and anonymous help to those with concerning or illegal internet use. They have helped thousands of people in this situation.

0808 1000 900 | help@stopitnow.org.uk | www.stopitnow.org.uk

If you think this page has been blocked in error please contact iwf@talktalkplc.com or visit: <http://www.iwf.org.uk/accountability/complaints/content-assessment-appeal-process>

3.4 We also work closely with CEOP, and our Chief Executive sits alongside CEOP on the UKCCIS Board. We fully cooperate with their requests for information under RIPA and are currently in discussions about other ways in which we could support their work further. We signpost customers to their helpline via the “Report Abuse” button that sits on our customer safety information centre.

3.5 We believe the issue of extremist material and material intended to promote terrorism or acts of violence is predominantly a matter for law enforcement agencies and should be addressed via a joined up, multi-pronged approach to tackling extremism and terrorism. As an ISP we adhere to requests to remove content that has been found to be illegal under current UK legislation. This may include material found to be extremist or material intended to promote terrorism or acts of violence. We are also in the process of finalising an agreement with the Home Office to include their filtering list of known terrorist websites that breach Terrorism Act 2006 but that the policing Counter Terrorism Internet Referral Unit have been unable to get taken down, for example because they are hosted abroad. We intend to add this into our “weapons and violence” category within HomeSafe, so that our customers can choose to filter access if they want.

4. PREVENTING ABUSIVE OR THREATENING COMMENTS ON SOCIAL MEDIA

4.1 Our own research supports that cyberbullying is one of the main concerns for parents and children alike when it comes to the internet and it is clear that more needs to be done both to prevent cyberbullying and support the victims. Predominantly however we believe that the issue of cyberbullying is a behavioural issue and therefore one that needs to be tackled through education, and then those websites owners and as opposed to action we can take technically as an ISP.

4.2 In terms of what we are able to do, we investigate any abusive or threatening comments, posted on sites by our customers when we are provided with the log information that supports the complaint. In these cases where we can, we will identify the account and contact the account owner to make them aware of the complaint. We inform the customer that this action is undertaken because of a breach of our Terms and Conditions of supply. Depending on the severity of the abuse, some cases may result in court action. In these instances, we would not contact the customer to make them aware, but we will disclose relevant data to the third party solicitor, on receipt of a fully sealed court order from a UK court.

4.3 We do provide customers with the option of blocking social media via HomeSafe however we do not think that this solves or helps the issue of cyberbullying. Our safety centre also includes a range of information about cyberbullying for parents and we signpost to organisations like BeatBullying for further support.

ABOUT TALKTALK GROUP

TalkTalk is the UK’s leading value for money TV, broadband and phone provider with 4 million customers across the UK. TalkTalk operates the UK’s largest Next Generation Network that covers 95% of UK homes. TalkTalk is one of seven partners behind YouView, the internet-connected TV service, along with the BBC, ITV, BT, Channel 4, Arqiva and Five. YouView launched to UK homes in 2012 and in August 2013 TalkTalk announced it had signed up over 500,000 customers to the service. TalkTalk is also the only provider to provide a whole home parental controls service, HomeSafe, to its customers free of charge. HomeSafe protects every device using the broadband from accessing inappropriate content and since launch has been activated by 1.2 million customers. TalkTalk Business has been a leading supplier of broadband and voice for almost 20 years

to over 180,000 businesses across the UK. TalkTalk is a founding partner of charity Go ON UK, which aims to make the UK the most digitally included nation in the world.

October 2013

Written evidence submitted by the Mobile Broadband Group

INTRODUCTION

1. The Mobile Broadband Group (“MBG”), whose members are the UK businesses of EE, Telefonica UK (O2), Three and Vodafone, welcomes the Culture, Media and Sport Select Committee’s Inquiry into online safety.

2. We also welcome the opportunity to submit information on the significant steps that the mobile operators have taken over the years, both individually and collectively, to mitigate risks that customers, particularly children, may face when accessing content and services on-line.

3. The mobile operators’ work in this area is underpinned by a Code of Practice that was first published nearly ten years ago in January 2004—“The UK code of practice for the self-regulation of new forms of content on mobile”. The second edition of the code was published in 2009 and the third (and current) edition in July 2013, reflecting the mobile operators’ determination to keep the code up to date and relevant to evolving market conditions.¹⁷

4. The Code was first published in anticipation of the mass take-up of new mobile devices with enhanced features, including colour screens, picture messaging, video cameras and Internet browsers. Today the majority of children have a mobile and an increasing proportion of them go online using a mobile phone or smart phone.¹⁸

5. The intention behind the Code is that parents and carers should have access to the information with which to show their children how to use mobile devices responsibly and the tools with which to influence the type of content accessible to children.

6. The Code was the first of its kind and was used as the boiler plate for similar codes introduced by mobile operators throughout the EU. The UK has thus made an enormous contribution to child safety in Europe and beyond in this field. It is a universal topic, where international co-operation can and must complement work done in the UK.

PROVISIONS OF THE CODE OF PRACTICE

7. The Code covers a broad range of topics: commercial and Internet content, illegal content, malicious communications, spam communications and customer education.

Commercial and Internet content

8. The mobile operators’ respective responsibilities for commercial content—where they have contractual agreements in place with content providers—as against general content on the Internet are different.

9. Commercial content is classified in accordance with a framework provided by an independent body and any content with an 18 rating is placed behind access controls. Such content is not made available to customers until they have been through a robust age verification process (acceptable methods of which are set out in the Code).

10. In 2013, the mobile operators appointed the British Board of Film Classification (BBFC) as the provider of the independent framework (replacing the Independent Mobile Classification Body). The agreement took effect on 2nd September 2013.

11. The mobile operators’ partnership with the BBFC, who have increasing expertise in the on-line arena, enables consistent, evidence based and transparent decisions about the categorisation of commercial content and the calibration of Internet filters.

12. The Code requires that the mobile operators offer a filter to customers. The BBFC’s role, on the basis of all relevant evidence, is to provide advice to mobile operators on where to set their Internet filters. The framework focuses on content that may be harmful for children (ie those under the age of 18) to view—such as pornography, violence, hate, promotion of suicide, illegal drugs and is set here: <http://www.bbfc.co.uk/what-classification/mobile-content/framework>.

13. The mobile operators, though, are not setting out to police the Internet or online providers. It is Government’s role to set and enforce societal standards. Providers of age restricted products such as gambling, weapons, publications and alcohol should still be putting in place their own processes to ensure that minors are not accessing, or taking delivery of, their restricted goods and services.

¹⁷ http://www.mobilebroadbandgroup.com/documents/UKCodeofpractice_mobile_010713.pdf

¹⁸ Ofcom, Children’s media use 2012

14. In addition to providing the independent standards framework, the BBFC has within its remit the ability to review complaints about whether or not particular websites should or should not be placed behind the filter and provide guidance to the mobile operators on the filtering of the sites that are the subject of the complaint. Where there have been instances of inadvertent or unfounded over-blocking, there is a quick and transparent process for having web-sites removed from filtering.

15. The BBFC framework is binary—18 or unrestricted. This is because 18 is the only age at which it is currently practical to implement convenient, ubiquitous and robust on-line age verification. Stricter filters are available in the market for parents that may want a narrower range of content for younger users but these fall outside the Code.

16. The “18” filter is set by default for prepaid phones on all networks. For contract phones, where the customer has to prove that he or she is at least 18, the filter is set to on by default for three of the four networks. The operator Three will also put the filter on by default in 2014.

Measuring effectiveness

17. Obtaining robust, quantitative research as to whether the approach has been effective at protecting children from harmful content is difficult, not least because of the practical problems associated with researching this topic with children.

18. Ofcom and the London School of Economics led EU Kids On-line project provide two potential sources of indicative information.

<i>Seeing things that make me feel sad, frightened or embarrassed (%)</i>			
	8–11	12–15	
TV	22	14	Fig 113
Internet	16	10	Fig 114
Mobile	10	5	Fig 119

Data from Ofcom “Children and Parents: Media Use and Attitudes Report”, October 2012¹⁹

Table 6: Child has seen sexual images online or offline in past 12 months, by age and gender (%)

	9–12		13–16	
	<i>Boys</i>	<i>Girls</i>	<i>Boys</i>	<i>Girls</i>
TV/film/video	10	7	22	23
On any web site	6	3	22	13
In magazine or book	6	3	18	13
On a mobile	0	0	12	8

Data from EU Kids online project—UK report²⁰

19. The MBG describes this data as only indicative of the effectiveness of filtering. It is not clear that content that “makes me feel sad, frightened or embarrassed” equates to harmful or inappropriate content. Children could be seeing age inappropriate (ie by reference to accepted standards of taste and decency) content that does not make them feel such emotions, and vice versa.

20. Children could also be seeing content on their mobiles that is not captured by the filtering systems—such as text and picture messages that are sent directly between individual customers or content that is accessed over networks outside the control of the mobile operators, such as domestic and public wi-fi. However, the providers of public and domestic wi-fi have made considerable progress recently on the provision of filters to cover all devices in public spaces and in the home and this should go some way to mitigating the risk of children accessing age inappropriate content on mobile devices through any network.

21. It is encouraging to note from the data that there is a degree of consistency between the two and that for both Internet and particularly mobile, the incidence of age inappropriate content being seen is far lower than for the regulated TV market. Anecdotally, from the hundreds of millions of contacts, both in store and on help-lines, between customers and the mobile operators’ across a very broad range of topics, only a small handful are raised in a situation where a customer has expressed concern about exposure to age inappropriate content.

22. The overriding impression is that children are being appropriately and effectively protected by the measures being taken.

ILLEGAL CONTENT

23. Mobile operators work with the Internet Watch Foundation (IWF) and law enforcement agencies to deal with the reporting of illegal child abuse imagery. If illegal content were to be identified on servers hosted by

¹⁹ <http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/oct2012/main.pdf>

²⁰ <http://eprints.lse.ac.uk/33730/7/Risks%20and%20safety%20for%20children%20on%20the%20internet%20-%20full%20report%20%28LSERO%29.pdf>

a mobile operator, including web or messaging content, it would be removed quickly, in accordance the relevant notice and take-down provisions. It is very rare to receive such a notice.

24. Mobile operators receive the IWF's list of URLs containing potentially illegal content and, in order to protect customers from being exposed to such content (and thus committing an offence), block the Internet browser from accessing any URL on the list. Any customer, inadvertently or otherwise, attempting to access such a site would be directed to a landing page explaining the reason that the page had been inaccessible (using one of the standard texts endorsed by the IWF).

MALICIOUS COMMUNICATIONS

25. Under the Code, the mobile operators commit to procedures for dealing with malicious communications that occur on their services (ie not third party platforms and services) and are reported to them. Mobile operators ensure that customers have ready access to mechanisms for reporting to them concerns (such as to a specialist nuisance calls desk). It is an offence to misuse electronic communications services and, where requested by law enforcement agencies, mobile operators can and do assist with the compilation of evidence against perpetrators.

UNSOLICITED COMMUNICATIONS (SPAM TEXT MESSAGES)

26. For a number of years, mobile operators have provided customers with a short code 7726 (the numbers for S-P-A-M on an alphanumeric keypad) to which unwanted texts can be forwarded. This provides vital early intelligence to MNOs, who can investigate the content and source of the messages.

27. In the current year, under the auspices of the global mobile trade body, the GSM Association, the UK mobile operators and the Information Commissioner have signed an MOU with a view to sharing intelligence about 7726 reports. This enhanced intelligence sharing is enabled through a trial of the new GSMA Spam Reporting Service.

28. In short, the platform provides a range of tools to analyse data being sent into the 7726 shortcodes of the UK mobile networks. Approximately 10–15k reports are received each week, resulting in approximately 500 SIM cards being disconnected weekly by the mobile networks.

29. A more detailed memorandum on this topic has been submitted to the Committee in relation to its inquiry into Nuisance calls and texts.

INFORMATION AND ADVICE

30. Mobile operators provide extensive advice to customers—including children, parents and carers—across a broad range of topics relating to the use of mobile devices and services, such as: privacy, security, Apps, billing, cost control, and all the matters covered by the content code. Mobile operators, through selected partnerships and other arrangements also support relevant media literacy activities by others which are designed to improve the knowledge of consumers in this area.

31. The mobile operators have demonstrated their commitment to customer safety by investing significantly in filtering and age verification processes over the last ten years—both in terms of capital expenditure and operating costs. We believe that our approach has been effective. But technical solutions are not foolproof and it remains essential that all channels of communication are used to raise awareness among parents and children of how best to stay safe online and how to behave appropriately.

DEVICE LEVEL FILTERING

32. Beyond matters that are within the Code (and the remit of the MBG), the mobile operators would like to see manufacturers continue to develop and improve the filtering and control mechanisms that are available on portable mobile devices such as smart phones.

33. At present, some of the filtering tools available can be quite blunt and may only offer an “on” or “off” ability to browse the Internet. With the increasing sophistication of operating systems for mobile devices, it should become possible for manufacturers to install software that will aid filtering and support more comprehensive solutions.

34. Software that enables the consumer to make more decisions about what the device can or cannot do, particularly when browsing the Internet, would enable them to have a much clearer sense of the level of protection they enjoy, and a greater ability to tailor protection to their own specific needs, independent of the network through which they are connected.

35. The mobile operators have had network filtering in place for nearly ten years. Great pressure has also recently been put on the domestic ISPs and public wi-fi operators to do the same—and this is happening. However, all these efforts would be complemented with the availability of better user controls at operating system and device level. The UK, through UKCCIS and other channels, should continue to examine closely what the manufacturers and operating system providers are offering in the area of child safety and challenge them to be as equally committed as the network providers.

DIGITAL SKILLS FOR LIFE

36. With the Government's focus on digital skills, and the move towards the online delivery of public services, it is important that children and adults are not afraid to use the Internet, and are equipped with the skills they need to become confident web users.

37. The Internet makes available a wealth of information, the lack of which can put people at a significant disadvantage in areas such as finding employment, housing, education, and making cost savings. With an estimated 7 million people still not using the Internet, with fear being one of the strongest reasons given for not going online, it is important that Government, industry and the media be supportive of these groups to encourage them to get online.

38. The mobile networks welcome the Government's changes to the education curriculum to enable children to learn, from an early age, digital skills, including coding, from primary school. It is vital, though, that online safety and wellbeing is taught as well, as part of the curriculum and across subjects. Teachers of all disciplines must be trained to teach the relevant skills and appropriate on-line behaviour and young people must be equipped to understand their responsibilities and how to respond if they ever feel uncomfortable whilst online.

39. There are also economic considerations. Research recently commissioned by Telefonica UK (O2) has estimated that the unused digital skills among the one million unemployed young people would be worth £6.7 billion²¹ to the UK economy. Those born into the digital generation will have strong digital skills including web design, coding and social media expertise. While business must do more to realise these benefits, these skills must be coupled with appropriate skills for staying safe and behaving responsibly while online.

40. The mobile operators therefore remain committed to maintaining the constructive cross-stakeholder work with Government, regulators, law enforcement agencies, charities and other interested parties to keep the UK at the forefront of the Internet safety agenda.

September 2013

Written evidence submitted by Facebook

SUMMARY

1. This submission sets out Facebook's policies and actions around safety to help inform the Committee's inquiry into these matters.

2. Facebook's mission is to make the world more open and connected and to give people the power to share. Facebook is a global community of more than 1.15 billion people and hundreds of thousands of organizations. Each person and organization that uses Facebook represents unique opinions, ideals and cultural values. With this immense diversity, we work to foster and safe and open environment where everyone can freely discuss issues and express their views, while respecting the rights of others.

3. The policies Facebook has adopted are designed to reflect real world interactions. While ignorance still exists both on and off of Facebook, we believe that ignorance will not be defeated by covering up its existence, but rather by confronting it head on.

4. We have learned that requiring people to engage in conversations and share their views using their real names and identities promotes an environment of accountability, where contributors must take responsibility for their own thoughts and actions.

5. Facebook's detailed Statement of Rights and Responsibilities ("SRR") describes the content and behaviour that is and is not permitted on our service. With respect to safety, our SRR specifically prohibits the following types of behaviours:

- (a) Bullying, intimidating, or harassing any user.
- (b) Posting content that: is hate speech, threatening, or pornographic; incites violence; or contains nudity or graphic or gratuitous violence.
- (c) Using Facebook to do anything unlawful, misleading, malicious, or discriminatory.

6. Further, Facebook encourages people to report content that they believe violates our terms. We have "Report" buttons on every piece of content on our site. When we receive a report, we have a dedicated team of professionals that investigate the piece of content in question. If the content in question is found to violate our terms, we remove it. If it does not violate our terms, then we do not remove it. We also take action, such as disabling entire accounts (eg of trolls) or unpublishing Pages, if deemed necessary.

7. We want everyone on Facebook to feel well-equipped to keep themselves safe when using the service. In particular, we have focused on educating our teenage users, their parents and teachers. We understand that younger users warrant additional protection and we work in partnership with external audiences to educate them on our safety tools.

²¹ <http://news.o2.co.uk/?press-release=young-peoples-digital-skills-valued-at-6-7billion-by-uk-businesses>

HOW WE COMBAT CHILD SEXUAL EXPLOITATION

8. Facebook has a zero tolerance policy for child exploitation and abuse and we fight against these activities aggressively. We employ advanced technology to protect minors on our site, and we deploy innovative, industry-leading measures to prevent the dissemination of child exploitation material. We have also built complex technical systems that either block the creation of this content altogether, including in private groups, or flag it for immediate review by our safety team.

9. For instance, in collaboration with Microsoft and the National Center for Missing and Exploited Children (“NCMEC”), we utilize a technology called PhotoDNA that allows us to instantaneously identify, remove and report known images of child exploitation content to NCMEC. PhotoDNA is a game-changing technology that has helped enormously in preventing the sharing of abusive materials on Facebook and other services. Once a piece of content is reported to NCMEC, NCMEC then coordinates with law enforcement authorities around the world to investigate and prosecute people who are creating and sharing these images online.

10. In the rare instance where child exploitation content is reported or identified by our users on Facebook (ie, if the content is a new image of abuse which is not already in our database of known images), we similarly, take it down as soon as possible and report it to NCMEC.

11. All related reports for the UK are referred to CEOP. CEOP is then able to evaluate each case and where appropriate, engage local police forces for further investigation and subsequent prosecution.

12. Additionally, we provide a dedicated escalation channel for the IWF and other Internet hotlines to inform us of illegal images being shared on Facebook,. It is a real testament to the effectiveness of our counter measures, and particularly PhotoDNA’s technology, that very few reports of such content are received from these hotlines in any 12-month period,

13. We also work hard to identify, investigate and address grooming behaviour—direct communication by an adult with a minor with the objective of illegal sexual contact. We work closely with law enforcement, external partners, expert academics and the Facebook community itself, to spot grooming and to combat it.

HOW WE KEEP PEOPLE SAFE

Handling reports

14. We have a comprehensive and well-resourced User Operations (“UO”) team that services all of our users twenty-four hours each day, seven days a week. This team handles every report that is submitted to Facebook (including by people who do not have a Facebook account). Hundreds of employees work on the User Operations team, which is located in four offices across the globe, namely Hyderabad (India), Dublin (Ireland), Austin (US) and Menlo Park (US). They handle reports in over twenty-four languages and cover every time zone. Structuring the teams in this manner allows us to maintain constant coverage of our support queues for all our users, no matter where they are in the world.

15. In order to effectively review such reports, UO is separated into four specific teams, which review different report types—(1) the Safety team, (2) the Hate and Harassment team, (3) the Access team, and (4) the Abusive Content team. When a person reports a piece of content, depending on the nature of the report, it will be directed to the appropriate team. For example, if you are reporting content that you believe contains graphic violence, the Safety Team will receive and assess the report.

16. If one of these teams determines that a reported piece of content violates our policies or our Statement of Rights and Responsibilities, we will remove it and warn the person who posted it. In addition, we may also revoke a user’s ability to share particular types of content or use certain features, disable a user’s account, or if need be, refer issues to law enforcement. We also have special teams dedicated to handle user appeals for instances where users feel Facebook might have made a mistake in taking a specific action. We recently published an infographic, which shows the processes involved in Facebook’s user operations for handling reports.²²

17. Further, we provide all users with a tool, “The Support Dashboard,” which is designed to give a user much better visibility and insight into the reports they make on Facebook. The Support Dashboard enables people to track their submitted reports and informs them about the actions taken by our review team. We think this will help people better understand the reporting process and will educate them about how to resolve their issues in the future. As people see which of their reports result in a removal of content, we believe users will be better equipped to make actionable reports. We posted about the Support Dashboard when we unveiled it in April 2012, on our Safety Page.²³

Keeping young people safe

18. We provide educational materials through our Family Safety Centre²⁴ which provides information for anyone interested in keeping children safe online. The Centre includes specific guidance for teenagers and also provides information about our global Safety Advisory Board.

²² <https://www.facebook.com/notes/facebook-safety/what-happens-after-you-click-report/432670926753695>

²³ <https://www.facebook.com/notes/facebook-safety/more-transparency-in-reporting/397890383565083>

²⁴ <http://www.facebook.com/safety>

19. Our Safety Advisory Board is comprised of five leading Internet safety organizations from North America and Europe. These organizations serve in a consultative capacity to Facebook on issues related specifically to online safety. The members of our Safety Advisory Board include the following:

- Childnet International.
- National Network to End Domestic Violence.
- Connect Safely.
- The Family Online Safety Institute.
- WiredSafety.

20. We maintain a Facebook Safety Page,²⁵ which has been “liked” by over one million people. All these fans can therefore see the latest information on safety education directly in their Facebook Newsfeeds. We regularly post information, tips, and articles about safety on Facebook and highlight debates on the topic of digital citizenship, as well as links to useful content from third-party experts.

Under 13s

21. It is well understood that, like many other online services, Facebook’s SRR requires users to be 13 to sign up for a Facebook account. We therefore require all users to provide their date of birth when signing up for Facebook to ensure that people under 13 are not able to open an account.

22. However, we are well aware of different studies in the UK and elsewhere that demonstrate how many under-13s are falsifying their ages to open accounts, often with their parents’ knowledge and even their help. There is no fail-safe way of addressing the issue of under-age users and we continue to explore best approaches to the issue with policymakers, our Safety Advisory Board, and our safety partners.

UK partnerships and schools

23. We work with a range of expert partners in the UK who go into schools to provide training and guidance for teachers, pupils and parents. We take a partnership approach because we have found it to be particularly effective. Organisations like Childnet, the South West Grid for Learning, the Diana Award (Anti-Bullying), Childline and Parentzone are trusted safety and advice brands, who are able to help schools and parents navigate the great variety of online services used by children including Facebook—from online games to mobile devices, from Twitter to Snapchat and Ask.fm.

24. We particularly support the work of Childnet and the South West Grid for Learning, which runs the InSafe hotline for professionals in education, and work directly in schools. In recent years, we have funded the production of thousands of Facebook guide booklets, which these organizations distribute widely. In November 2012 we launched an anti-bullying initiative in partnership with Childline, which encouraged bystanders to take action when they saw others being bullied.

25. We participate and support the annual “Safer Internet Day” run by the UK Safer Internet Centre, which comprises these two organisations and the IWF.

26. Facebook was the principal sponsor of The Festival of Education at Wellington College in June 2013. The Festival is the biggest gathering of its kind in the UK with over 2,500 delegates attending. Over 500 different schools, colleges and universities were represented at the Festival. In addition to these delegates, more than 600 pupils from over 50 schools took part. At the Festival, the Education Foundation partnered with us to launch an updated Facebook Guide for Educators.²⁶ This guide provides up-to-date advice on privacy and safety topics as well as a general introduction to Facebook. The guide features two pilot programmes where Facebook has been used for learning in two different schools, the Wellington College and the Nautical School in London. A short film summarising the work was premiered at the Festival (see link on the Education Foundation website). A copy of the Facebook Guide was provided to every attendee at the Festival and is also available to download for free from the Education Foundation website.

27. We will continue to partner with these and other relevant organisations over the coming months and years to help equip young people, teachers and parents with the best information and tools they need to promote online safety and healthy digital citizenship.

September 2013

²⁵ <http://www.facebook.com/fbsafety>

²⁶ <http://www.ednfoundation.org/2013/06/21/facebook-guide-for-educators/>

Written evidence submitted by Twitter

INTRODUCTION

1. Twitter is an open, public platform built around small bursts of information, which we call Tweets. Each Tweet can be no more than 140 characters long. In addition to text, Tweets can include photographs, videos, or links. Users can control their experience on the platform by choosing who to follow and what they wish to see.

THE TWITTER RULES

2. Twitter provides a global communication service which encompasses a variety of users with different voices, ideas and perspectives. With 200 million active users across the world and 15 million in the UK alone, the platform now serves 500 million tweets a day. Like most technology companies we are clear that there is no single silver bullet for online safety, rather it must be a combined approach from technology companies, educators, governments and parents to ensure that we equip people with the digital skills they will need to navigate the web and wider world going forward.

3. As a general policy, we do not mediate content. However, there are some limitations on the type of content that can be published with Twitter. These limitations comply with legal requirements and make Twitter a better experience for all. These limitations include prohibitions on the posting of other people's private or confidential information, impersonation of others in a manner that does or is intended to mislead, confuse, or deceive others, the posting of direct, specific threats of violence against others, and trademark and copyright infringement.

4. Our rules and terms of service clearly state that the Twitter service may not be used for any unlawful purposes or in furtherance of illegal activities. International users agree to comply with all local laws regarding online conduct and acceptable content.

5. Full details of Twitter's rules and terms of service be found in our support centre: <https://support.twitter.com/articles/18311-the-twitter-rules>

ILLEGAL CONTENT—CHILD SEXUAL EXPLOITATION POLICY

6. We do not tolerate child sexual exploitation on Twitter. When we are made aware of links to images of or content promoting child sexual exploitation they will be removed from the site without further notice and reported to The National Center for Missing & Exploited Children ("NCMEC"); we permanently suspend accounts promoting or containing updates with links to child sexual exploitation.

7. We have established a line of communication and maintain an ongoing dialogue with the Child Exploitation and Online Protection Centre, both in relation to its investigative work and also in its important work around education and awareness raising. Twitter is also a member of the Internet Watch Foundation.

8. We are in the process of implementing Photo DNA into our backend technologies and, like other technology companies, are engaged with law enforcement and non-governmental organisations on global efforts to track and eliminate child abuse images online.

9. Twitter is part of the technology task force for Thorn (<http://www.wearethorn.org>), a cross industry foundation which aims to disrupt the predatory behavior of those who abuse and traffic children, solicit sex with children or create and share images of child sexual exploitation. Thorn exists to continue the work started by the Demi and Ashton (DNA) Foundation in 2009.

10. In the rare instance that a user finds a Twitter account which they believe to be distributing or promoting child sexual exploitation while using Twitter, they are asked to notify us by sending an email to cp@twitter.com. They are also asked *not* to Tweet, retweet or repost child sexual exploitation for *any* reason and rather to report it to us immediately so we can take steps to remove it.

ONLINE SAFETY

11. Twitter provides a global communication platform which encompasses a variety of users with different voices, ideas and perspectives. As stated above, the platform now serves 500 million tweets a day.

12. Our policy is that we do not mediate content or intervene in disputes between users but we do have a clear set of rules which govern how people can behave on our platform. These rules are designed to balance offering our 200 million global users, a service that allows open dialogue and discussion all around the world whilst protecting the rights of others. As such, users may not make direct, specific threats of violence against others; targeted abuse or harassment is also a violation of the Twitter Rules²⁷ and Terms of Service.²⁸

13. To help users navigate issues they may be confronted with online, we offer a number of articles in our Safety and Security Centre²⁹ that guide users to make better decisions when communicating with others.

²⁷ <http://support.twitter.com/entries/18311#>

²⁸ <https://twitter.com/tos>

²⁹ <https://support.twitter.com/groups/57-safety-security#>

14. Over the course of the next months, we will be publishing new content with more information, including local resources provided by our partners in the safety community across the world. Some of the new content will be aimed at bystanders—those who may witness abusive behavior, but are not sure what actions to take. Teaching users to help each other as well as knowing when and how to contact Twitter for help is vital to Twitter being a safe space for our users.

15. We also work with a number of safety organizations around the world to provide content to our users that may be useful for navigating problems online, and plan to host more content from them and other safety experts in future iterations of the site.

16. We often use the analogy of Twitter as a public town square where users are free to speak with and interact with others; that said, just as in a public town square, there are behaviors that are not allowed.

17. In addition to reporting violations of our Terms of Service and Rules, users can control what content they see through features like blocking and sensitive media warnings. When our users see or receive an @reply they don't like, they can unfollow the author of the Tweet (if they are following the user), which will remove that user from their home timeline. They can also block the user³⁰ which will mute the communication. When you block a user you will not be notified when they mention you, retweet you, favourite your content, add you to a list or subscribe to one of your lists. You also won't see any of these interactions in your timeline. This prevents you from receiving unwanted, targeted and continuous @replies on Twitter. Abusive users often lose interest once they realize that their target will not respond.

18. Another option available to our users is to protect their accounts.³¹ Users with protected accounts can approve requests from other users to follow their accounts on a case-by-case basis. Additionally, their tweets are only viewable and searchable by themselves and their approved followers. As such, they can prevent any unwanted followers from viewing their content.

19. Sometimes users see content they don't like in the form of images or video, and for that we have settings that allow users to label their media for the appropriate viewers, and select whose media will display on their own Twitter homepage. We ask users to mark their Tweets as sensitive if they contain media that might be considered sensitive content such as nudity, violence, or medical procedures.

20. For the viewer, the default setting is that if a Tweet is marked as containing media that might be sensitive, they will be required to click through a warning message before that media is displayed to them.

21. If another user notices that Tweets have not been marked appropriately, that user may flag the image or video for review. The content will then be reviewed and a determination made as to whether that media requires an interstitial in order to comply with Twitter's Media Policies.³²

22. We are continuing to expand our user support and safety teams to ensure we are supporting our growing userbase appropriately. We also continue to invest heavily in our reporting system from a technological perspective and recently rolled out a significant update which simplified our system, allowing people to report violations³³ to us via an in-Tweet reporting button as well as via the forms in our support centre.³⁴

23. Once a user files a report to Twitter, they are sent a ticket number and the form is routed to a team of trained reviewers. If accounts are found to be acting in way which breaks our rules, for example posting specific threats, then we take action, up to and including suspending accounts. At the end of the process the specialist reviewer follows up with the person who filed the ticket to let them know that their report has been addressed.

24. Reports that are flagged for threats, harassment or self-harm are reviewed manually. We also use automated tools to help triage reports filed for other types of complaints, such as spam.

25. It is important to stress that where a user believes the content or behavior he or she is reporting is prohibited by law or if they are concerned for their physical safety, we advise them to contact local law enforcement so they can accurately assess the content or behaviour. If Twitter is then contacted directly by the Police, we can work with them and provide assistance for their investigation.

26. Twitter works closely with UK law enforcement. We have updated our existing policies around handling non-emergency requests from UK law enforcement to more closely mirror our process for US-based law enforcement requests (including providing notice to users). We have always responded to emergency disclosure requests from law enforcement in situations involving danger of death or serious physical injury to any person.

27. Twitter invokes these emergency disclosure procedures in the United Kingdom if it appears that there is an exigent emergency involving the danger of death or serious physical injury to an individual. Twitter may provide UK law enforcement with user information necessary to prevent that harm.

³⁰ <https://support.twitter.com/articles/117063#>

³¹ <https://support.twitter.com/articles/14016-about-public-and-protected-tweets#>

³² <https://support.twitter.com/articles/20169199-twitter-media-policy#>

³³ <https://support.twitter.com/articles/15789-how-to-report-violations#>

³⁴ <https://support.twitter.com/forms>

28. Twitter has published Guidelines for Law Enforcement (“Guidelines”; <https://t.co/leguide>) as well as a webform (<https://t.co/leform>) through which UK Law Enforcement can file a request or make an inquiry

29. Since opening our UK office, Twitter has worked to build relationships with stakeholders in the online safety sector. Twitter is a member of UKCCIS. The company has also established a single point of contact for the UK Safer Internet Centre and has worked with the South West Grid for Learning.

30. We participated in Safer Internet Day for the first time in 2012 implementing our “Tweets for Good” programme whereby we promoted safety messaging on the platform. We will continue this involvement and our work with our safety partners and wider voluntary organisations into the future.

September 2013

Written evidence submitted by Ofcom

SECTION 1

One page summary

1.1 Ofcom welcomes the opportunity to contribute to the Committee’s inquiry on online safety.

1.2 This document sets out Ofcom’s current duties and powers relevant to the Committee’s inquiry. It also describes what we consider to be some relevant market and consumer developments captured by our research that may assist the Committee.

1.3 The Committee’s inquiry considers three specific issues relating to online safety across a broad range of media services. In order to identify how we may be able to assist the Committee in future, we have structured our response to consider each of the three issues in turn; and for each we have described Ofcom’s relevant duties and/or role across the following services:

- Broadcast television and radio.
- ATVOD notified on-demand services.
- Online content more broadly.

Main conclusions of this document:

1.4 The internet has brought significant benefits to consumers and citizens and made the media a much more social, global and participative environment. However, the internet also brings new regulatory challenges. The connected environment and changes in consumer behaviour can result in audience protection risks and in particular, new challenges in securing the protection of children from potentially harmful content.

1.5 In a connected society there is particular pressure on consumers’ understanding of the increasingly complex regulatory environment, of the practices they can expect of service providers and of their awareness of their own responsibilities.

1.6 There is a task for the Government, regulators and industry to ensure the provision of clear information, education and a framework of personal responsibility through which individuals and families can exercise an informed choice.

1.7 Any approach to online safety should include a combination of the traditional content standards protections and industry-led measures which provide the right framework of information, online safety tools and content controls for audiences to protect themselves and their families.

1.8 It is important for consumers that online safety tools and content controls are easy to use and made available in as many internet connected devices as possible. Consumers should also be adequately informed of where such tools can be used.

1.9 The effectiveness and impact of online safety tools and content controls will, however, depend on actions being taken by individuals and parents. Therefore, in order to ensure potentially harmful content is subject to comprehensive oversight, further consideration may be needed as to the roles and responsibilities of all industry players in the online environment.

SECTION 2

Regulatory context

2.1 As the United Kingdom’s independent regulator for the communications sector, Ofcom’s principal duty in carrying out our functions (set out in section 3(1) of the Communications Act 2003) is:

- (b) to further the interests of citizens in relation to communications matters; and
- (c) to further the interests of consumers in relevant markets, where appropriate by promoting competition.

Television and Radio

2.2 In carrying out this duty, Ofcom has other statutory duties and powers relevant to the Committee's areas of inquiry. In particular, Section 3(2) of the Communications Act 2003 states that Ofcom is required to secure:

- The application, in the case of all television³⁵ and radio services, of standards that provide adequate protection to members of the public from the inclusion of offensive and harmful material in such services; and
- The application, in the case of all television and radio services, of standards that provide adequate protection to members of the public and all other persons from both:
 - unfair treatment in programmes included in such services; and
 - unwarranted infringements of privacy resulting from activities carried on for the purposes of such services.

2.3 All of Ofcom's decisions must comply with the Human Rights Act 1998 which incorporates into UK law the European Convention on Human Rights. Of particular relevance to Ofcom's decisions are: the right to a fair trial (Article 6), the right to privacy (Article 8) and the right to freedom of expression (Article 10). We are also subject to the Freedom of Information Act 2000.

2.4 Ofcom is also required to set standards in relation to TV and radio advertising.³⁶ Ofcom established a co-regulatory partnership with an industry body, the Advertising Standards Authority ("ASA"), in 2004. The arrangements are underpinned by an enabling statutory instrument³⁷ and a Memorandum of Understanding.³⁸

2.5 Although Ofcom has devolved the exercise of this function to the ASA (in this case, through an Order made under the Deregulation and Contracting Out Act 1994), it remains ultimately responsible for ensuring that broadcasters observe relevant standards.

2.6 Television services are provided over different platforms: digital terrestrial wireless transmission, via satellite, cable or over the internet. Under Article 2 of the AVMS Directive, a broadcast service will fall within the UK's jurisdiction if it is either based in the UK, either editorially or by other measures. If a service has no presence in the UK or EU then secondary technical criteria are used to determine jurisdiction, which includes the location of the satellite uplink.

Video on Demand

2.7 The Communications Act makes provisions for the regulation of on-demand programme services (ODPS), which are essentially services whose principal purpose is the provision of programmes the form and content of which are comparable to the form and content of programmes normally included in television services, ie TV-like video on demand (VOD) services. These services can be made available on any platform and are subject to a notification scheme if the editorial control of the service is generally based in the UK. Notified ODPS must comply with minimum content standards under the AVMS Directive, which has been implemented in the UK by Part 4A of the Communications Act 2003.

2.8 Ofcom has formally designated the Authority for Television On Demand (ATVOD) as the co-regulator for editorial content,³⁹ and the ASA as the co-regulator for advertising content. Ofcom remains ultimately responsible for ensuring that providers of on-demand services observe relevant standards.

Online

2.9 Our role in relation to internet services is much more limited. We regulate television channels delivered over the internet and notified ODPS when they are established in the UK; but we have no statutory powers to regulate any other online content. Ofcom also has media literacy duties which address media consumption online. These are detailed below, along with some information on further roles Ofcom conducts in relation to online services.

2.10 Section 11 of the Communications Act 2003 places a responsibility on Ofcom regarding the promotion of media literacy. We fulfil this duty through the publication of Media Literacy research into adults' and children/parents' media use and attitudes. We publish two substantial annual reports: "Children and Parents: Media Use and Attitudes" and "Adults Media Use and Attitudes". These provide detailed evidence of media use, attitudes and understanding among adults and among children and young people aged 3–15. The children's report also provides evidence of parents' concerns about their children's media use and the ways that they seek to monitor and mediate that use. Ofcom also publishes a range of other consumer research, exploring similar

³⁵ Under 232 (2) of the Communications Act 2003, a service falls within a "television licensable content service" if it **E+W+S+N.I.** This sectionnoteType=Explanatory Notes has no associated (a) is provided (whether in digital or in analogue form) as a service that is to be made available for reception by members of the public; and (b) consists of television programmes or electronic programme guides, or both.

³⁶ See section 321 Communications Act 2003.

³⁷ The Contracting Out (Functions Relating to Broadcast Advertising) and Specification of Relevant Functions Order 2004.

³⁸ http://stakeholders.ofcom.org.uk/binaries/consultations/reg_broad_ad/statement/mou.pdf.

³⁹ <http://stakeholders.ofcom.org.uk/binaries/broadcast/tv-ops/designation180310.pdf>.

themes. We share the findings of our research widely, including with the Government, industry, academia and the third sector.

2.11 Ofcom also has a seat on the Executive Board of the UK Council for Child Internet Safety (UKCCIS)⁴⁰ which brings together more than 200 organisations across the government, industry, law enforcement, academia and charity sectors, who work in partnership to help keep children safe online. Ofcom provides its research data to UKCCIS to help inform debates about these areas and has been involved in a number of UKCCIS initiatives, for example: the “Advice for Child Internet Safety 1.0—universal guidelines for providers”⁴¹; and the “Good practice guidance for providers of social networking and other inter-active services”.⁴²

2.12 In addition, the Government has recently proposed, through its published communications strategy paper “Connectivity, Content and Consumers—Britain’s digital platform for Growth”,⁴³ that it expects industry across the internet value chain “to ensure that all internet-enabled devices, whether a TV, a games console or a smart phone, are supplied with the tools to keep children safe as a standard feature”. The Government has asked Ofcom to have a role in overseeing this work and we are currently awaiting further details on this.

2.13 Ofcom was also significantly involved in developing ParentPort, which is a website with the single aim of protecting children by helping parents make their views heard about inappropriate programmes, advertising, products and services.⁴⁴ The website makes it easier for parents to complain about material they have seen or heard across the media, communications and retail industries.

SECTION 3

Market context and consumer context

3.1 Ofcom carries out research which informs the delivery of our duties and our programme of work. It also keeps us, and others, informed about new technology developments and the impact these may have on the sectors that we regulate. This section provides a brief overview of Ofcom’s observations on the effects of convergence on the way consumers and industry engage with media, and the challenges this may create for audiences.

3.2 Ofcom publish three reports that are of particular relevance to the Committee’s inquiry:

- The UK and Nations’ Communications Market Report,⁴⁵ last published in August 2013;
- Ofcom annual report “Children and Parents: Media Use and Attitudes”⁴⁶; and
- Ofcom annual report “Adults Media Use and Attitudes”.⁴⁷

3.3 Below we have set out a summary of these reports and you can find the full findings using the links provided above. Ofcom would also be pleased to provide a deeper and wider ranging discussion of our evidence base should the Committee require it.

Technology continues to evolve rapidly, resulting in an increasing range of new connected devices and changing consumption of AV content services

3.4 UK household internet access rose to 80% in Q1 2013, just one percentage point higher than in Q1 2012. However, mobile internet access rose ten percentage points to 49% of adults, the second fastest growth on record.

⁴⁰ <http://www.education.gov.uk/childrenandyoungpeople/safeguardingchildren/b00222029/child-internet-safety>

⁴¹ <http://media.education.gov.uk/assets/files/ukccis%20advice%20on%20child%20internet%20safety.pdf>

⁴² <http://media.education.gov.uk/assets/files/industry%20guidance%20%20%20social%20networking.pdf>

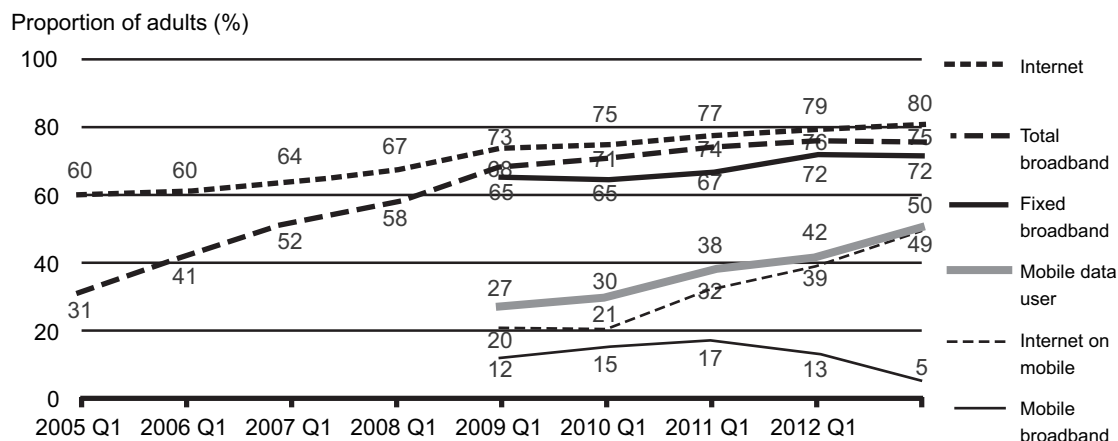
⁴³ https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/225783/Connectivity_Content_and_Consumers_2013.pdf

⁴⁴ www.parentport.org.uk. ParentPort has been jointly developed by the Advertising Standards Authority (ASA), the Authority for Television On-demand (ATVOD), the BBC Trust, the British Board of Film Classification (BBFC), Ofcom, the Press Complaints Commission (PCC) and the Video Standards Council (VSC)/Pan-European Game Information (PEGI).

⁴⁵ <http://stakeholders.ofcom.org.uk/market-data-research/market-data/communications-market-reports/cmr13/>

⁴⁶ <http://stakeholders.ofcom.org.uk/market-data-research/media-literacy-pubs/>

⁴⁷ <http://stakeholders.ofcom.org.uk/market-data-research/media-literacy/media-lit-research/adults-2013/>

Figure 3.1**HOUSEHOLD INTERNET ACCESS: 2005–2013**

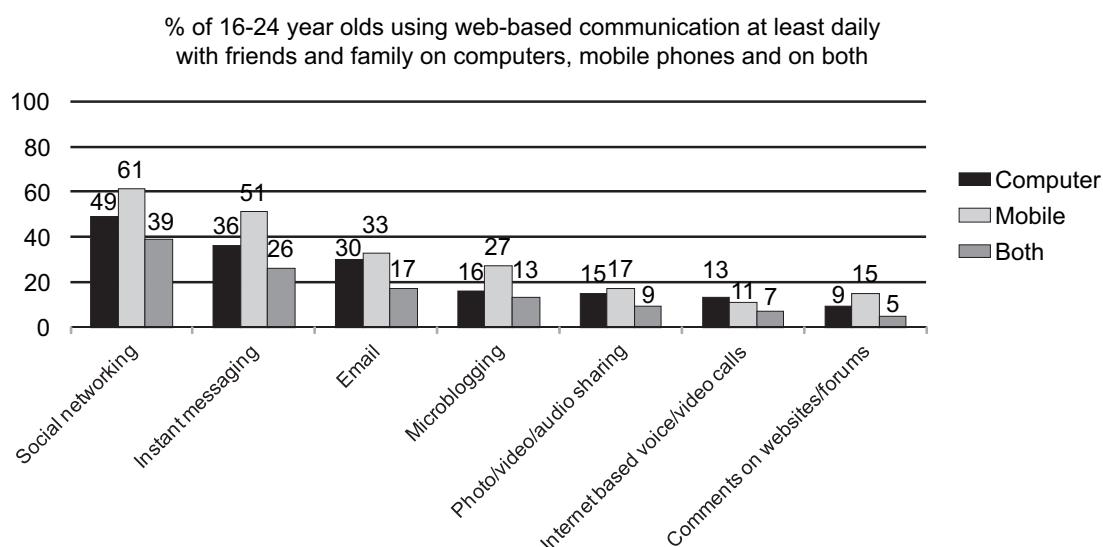
Source: Ofcom technology tracker, Q1 2013. Base: All adults aged 16+ (n=3750).

3.5 The power and functionality of devices connected to the internet are making them increasingly attractive to consumers, especially the scope that they give consumers to access, create and share content across different devices. The majority of devices continue to grow in terms of penetration.

3.6 There has been a particularly remarkable growth in the use of tablets. In spite of their relative novelty, in February 2013 tablets accounted for 8% of web-page views, double the level in 2012. Tablets are viewed as the main method of connecting to the internet by a third of users and just over half (56%) of tablet owners use their device for watching audio visual content.⁴⁸

There are increasing levels of take-up and usage of internet delivered services

3.7 There continues to be a demographic split in use of the internet. Younger people are more likely than older people to use the internet for activities related to converged media and this becomes more marked the older the age bracket. Conversely, younger people are more likely to access their media simultaneously meaning that, while they are consuming a greater volume of media than older people, they are doing so in a shorter time-period.⁴⁹

Figure 3.2**WEB-BASED COMMUNICATION ON COMPUTERS, MOBILE PHONES, AND BOTH, AMONG 16–24 YEAR OLDS**

Source: Kantar Media Omnibus

Base: All 16–24s in UK (N=375)

Q.2A How often do you use [insert statement] to communicate with friends and family?

⁴⁸ Ofcom Communications Market Report 2013. 51.

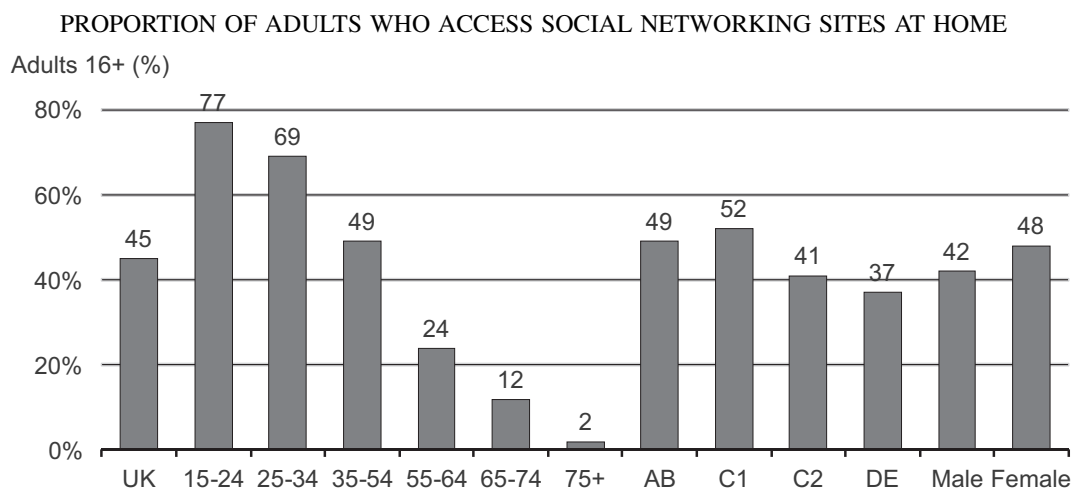
⁴⁹ <http://stakeholders.ofcom.org.uk/binaries/research/811898/consumers-digital-day.pdf>

Computers were defined as desktop PC, laptop, netbook or tablet

3.8 There is also evidence of growth in online video consumption. YouTube in particular has experienced strong growth in the last year with three quarters (74%) of laptop and desktop internet users visiting YouTube. Its unique audience grew 4% in the year to May 2013.⁵⁰

3.9 One of the key observable trends in web content consumption has been the rise of social networking, in particular among young people. Three-quarters of 15–24 year olds use social networking sites.

Figure 3.3



Source: Ofcom Consumer Research Q1 2013

Base: All adults aged 16+ (n = 5812 Q1 2008, 1581 Q3 2008, 6090 Q1 2009, 9013 Q1 2010, 3474

Q1 2011, 3772 Q1 2012, 3750 Q1 2013) QE5. Which, if any, of these do you use the internet for?

NB Question wording for QE5 prior to 2013 asked about household use of the internet at home.

In 2013 QE5 asked about individual use of the internet anywhere.

Consumers continue to have a high expectation for content standards on their television

3.10 In February 2012, Ofcom published a deliberative research report entitled “Protecting audiences in a converged world”.⁵¹ The research looked at public attitudes within the context of convergence, in order to understand the public’s expectations for protection and how content should be regulated in the future.

3.11 This research indicated that knowledge of prevailing content regulation is currently high for broadcast services but lower for other services (such as catch-up and VOD). The research also suggests that viewers have high expectations of content regulation on broadcast television, and associated VOD and catch-up services. Converged or connected TVs, which incorporate broadcast, VOD and open internet services, are considered to be closer to a TV-like experience. Audiences therefore expect content over these devices to be regulated more similarly to broadcast TV, in contrast to internet content accessed through devices such as PCs and laptops.

Parents are adapting the way they protect their children from certain kinds of content in light of technological change

3.12 Ofcom’s annual reports “Children and Parents: Media Use” and “Adults Media Use and Attitudes” provide detailed evidence of media use, attitudes and understanding among adults aged 16 and above and among children and young people aged three–15. Below are some of the key findings from the 2013 Adults⁵² and Children and Parents research.⁵³

3.13 In 2012 79% of households (aged 16+) had internet access, this is in line with 2011. The use of devices to go online at home, as seen among children, is diversifying with PC/laptop/netbook use remaining stable at 74%, although there were significant increases seen using other devices to access the internet at home. Mobile phone⁵⁴ access increased to 53% (up from 45% in 2011), tablet (16% vs. 6%) and games console (16% vs. 11%).

3.14 In 2013 91% of children aged five–15 live in a household with access to the internet through a PC, laptop or netbook and Ofcom’s research shows that children’s patterns of media consumption are changing.

⁵⁰ Ofcom commissioned qualitative research earlier this year to give us a better insight into the complex and diverse phenomenon of UGC. This provides a snapshot of the different players, types of content, business models and opportunities in this sphere. <http://stakeholders.ofcom.org.uk/binaries/research/research-publications/content.pdf>

⁵¹ <http://stakeholders.ofcom.org.uk/binaries/research/tv-research/946687/Protecting-audiences.pdf>

⁵² Adults’ media use and attitudes report 2013 (<http://stakeholders.ofcom.org.uk/market-data-research/media-literacy/media-lit-research/adults-2013/>)

⁵³ The Media Literacy research for 2013 is due to be published in October 2013.

⁵⁴ Mobile phone access includes smartphones. Personal smartphone use increased in 2012 from 44% to 54%.

Children are also increasingly likely to use a wide range of portable and personal devices, particularly smartphones and tablets. In 2013 43% of children aged five—15 owned a mobile phone with 62% of 12–15s owning a smartphone. Parents' ability to monitor what their children are doing online is becoming more limited than it was when internet access took place at a fixed point in the heart of the family home.

3.15 Among adult internet users over half (55%) say they use the same passwords for most websites. A quarter (25%) of users said they had problems remembering passwords, and a similar proportion (26%) said they tend to use easy to remember passwords like birthdays or names.

3.16 For adults, take-up of Wi-Fi protection and experience of deleting cookies from the web browser have increased since 2011. Very few internet users say they do not use online security measures or safety features because they don't know how they work, although a significant minority of people are unaware of a range of security features. Awareness and take-up of the security measures we asked about is typically lower among older users, DE adults and women.

3.17 43% of parents of children aged five—15 said that they use technical parental controls packages for desktop PCs, laptops and netbooks.⁵⁵ Uptake of controls for television is slightly higher at 45%. Use of filters on mobile phones where the phone can be used to go online is at 42% while uptake for controls on mobile/fixed games consoles is 16% and 19% respectively.

3.18 Parents generally view controls as an extra tool to supplement rather than a replacement for parental mediation (rules, monitoring and talking to children). 79% of parents of five—15 year olds have spoken to their child about staying safe online and just over half of parents have rules in relation to parental supervision. Overall, 85% of parents employ some kind of online mediation strategy to help their child stay safe online.

3.19 Other findings from the 2013 survey show that in households where five—15s use a PC/laptop or netbook at home 62% have some kind of technical method of control in place. 44% have safe search settings on search engine websites; 43% have parental controls⁵⁶ installed; 19% have the Safety Mode set on YouTube; 11% have software to limit the time spent online; 8% have a PIN/password set on broadcasters' websites. The most common reason reported by parents of older children (12–15) for not using access controls was that they trust their child to be sensible/responsible; and parents of younger children (five—sevens and eight—11s) are more likely to say it is because their child is supervised, or that the child is too young for a lack of controls to be a problem.

3.20 The majority of parents (79%) report that they know enough to keep their child safe online, but around half of parents continue to feel that their child knows more about the internet than they do, including 14% of parents of children aged three—four. Also, parents of eight—11s are more likely to agree with this statement now than in 2012 (44% vs. 35%).

SECTION 4

Protecting minors from accessing adult content

4.1 We have significant experience of regulating content that is unsuitable for children on broadcast television and radio services. Through our co-regulatory relationship with ATVOD we also have experience of regulating adult content on notified video on demand services. This section sets out details of some of our experiences of regulating this type of content on these services, which may be useful for the Committee. While Ofcom has no statutory role to regulate online services to protect children from accessing adult content, outside of television channels delivered on the internet and notified ODPS, this section also sets out some relevant research findings regarding adults' and children/parents' media use and attitudes that complements our understanding of this sector.

Ofcom's experience of regulating television and radio broadcast services

4.2 Under Section 319(1) of the Communications Act 2003, Ofcom has a statutory duty to set standards for broadcast content as appear to it best calculated to secure the standards objectives. These standards are set out in Ofcom's Broadcasting Code ("the Code") in the form of rules which broadcasters must comply with. These standards objectives include: "that persons under the age of eighteen are protected".

4.3 Ofcom considers the standards it has set for the protection of children, as set out in Section One of the Code, to be amongst the most important. The Code includes rules which help ensure the protection of minors from harmful content and from material that is unsuitable for them (covering content such as drugs, smoking, alcohol, violence and dangerous behaviour, and offensive language).⁵⁷ It also has rules that specifically relate to protecting children from sexual material, including prohibiting the broadcast of material equivalent to the

⁵⁵ This figure includes all available technical parental controls, for example parental controls provided by the ISP, but also parental controls built into the computer's operating system (windows or Mac), and third party parental controls such as net nanny or family shield.

⁵⁶ This includes parental controls provided by ISPs, the computers own operating system, or controls such as McAfee loaded by other people in the household.

⁵⁷ <http://stakeholders.ofcom.org.uk/broadcasting/broadcast-codes/broadcast-code/protecting-under-18s/>

British Board of Film Classification (BBFC) R18 rating and requiring “adult-sex material”⁵⁸ to be shown only between 10pm and 5.30am and behind mandatory restricted access.⁵⁹

4.4 Ofcom has sanctioned a number of adult-chat broadcasters for broadcasting sexually explicit material without the relevant protections.⁶⁰ For example, in November 2010 Ofcom imposed a financial penalty on Bang Channels and Bang Media (London) Ltd totalling £157,250 in respect of multiple breaches of the Code and licence conditions by the adult chat and daytime programming on these services. Ofcom concluded that the licensees had been operating a wholly inadequate compliance system which amounted to manifest recklessness. Ofcom revoked all the licences held by these licensees on the basis that they were no longer fit and proper to hold those licences.⁶¹

Ofcom’s experience of co-regulation for on-demand content

4.5 ATVOD has published Rules and Guidance to ensure compliance of all notified ODPS with certain minimum standards.⁶² Rule 11 of the ATVOD Rules reflects section 368E(2) of the Communications Act and states that, “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”.

4.6 ATVOD has adopted a precautionary approach to its interpretation of the wording of the Act and includes R18 material (or material equivalent to content classified in that category) as “material that might seriously impair”. Therefore R18 material or R18-equivalent content should only be made available in on-demand programme services in a manner which secures that persons under the age of eighteen will not normally see or hear it.

4.7 In the past year Ofcom has imposed financial penalties on three ATVOD notified ODPS for a breach of Rule 11. These sanctions were imposed on the services “Playboy TV”,⁶³ “Demand Adult”⁶⁴ and “Strictly Broadband”⁶⁵ after these services provided R18 equivalent material without adequate measures in place—a content access control system—to ensure that those under 18 would not normally see or hear it.

Relevant research findings regarding online services

4.8 Paragraphs 3.12 to 3.20 set out some relevant research findings from Ofcom’s recent Media Literacy research into adults’ and children/parents’ media use and attitudes, which looks at the behaviour and experiences of children and parents online.

4.9 Our research indicates that the majority of parents use a combination of mediation strategies to help keep their children safe online. Over four in 10 parents have parental controls installed, and feel that their children are safer as a result.

4.10 Most parents report that they know enough to keep their child safe online, but around half of parents continue to feel that their child knows more about the internet than they do, including 14% of parents of children aged 3–4. This may reflect the fast pace of technological change and the ease which younger children in particular can embrace and explore new mobile technology and apps and suggests that parents need continuing support to build their own skills and confidence.

4.11 Our research also shows that despite the vast majority of young people stating that they are confident internet users and that they know how to stay safe online, there is an increase in 12–15s undertaking risky activities online. A substantial minority of 12–15s have a social networking profile which may be visible to people not known to them and this has increased since 2012 (33% vs 22%). These children are more likely to be in the 15% who have undertaken some kind of potentially risky online behaviour such as adding people that they don’t know in person or sending photos or personal details to people only known online.

4.12 Some of these activities may be difficult to manage through technical controls; this reinforces the importance of developing children’s media literacy skills—to help them analyse and assess content, and manage the potential risks and unintended consequences of online activity—irrespective of technological changes.

4.13 How to protect children from the risk of exposure to harmful content online is an issue that has been closely considered by UKCCIS. There are already examples of industry-led approaches to support the protection of minors from such content. For example: all major ISPs provide customers with parental control software either for individual devices or for the whole home, via network-layer filtering. All major ISPs recently committed to offering their customers a network-layer filtering option and search providers offer “safe”

⁵⁸ Material that contains images and/or language of a strong sexual nature which is broadcast for the primary purpose of sexual arousal or stimulation.

⁵⁹ Mandatory restricted access means there is a PIN protected system (or other equivalent protection) which cannot be removed by the user, that restricts access solely to those authorised to view.

⁶⁰ <http://stakeholders.ofcom.org.uk/enforcement/content-sanctions-adjudications/?pageNum=1#in-this-section>

⁶¹ <http://stakeholders.ofcom.org.uk/binaries/enforcement/content-sanctions-adjudications/bangmedia-revocation.pdf>

⁶² Under the AVMS Directive, which has been implemented in the UK by Part 4A of the Communications Act 2003.

⁶³ http://stakeholders.ofcom.org.uk/binaries/enforcement/vod-services/Playboy_TV_Sanction.pdf

⁶⁴ http://stakeholders.ofcom.org.uk/binaries/enforcement/vod-services/Demand_Adult.pdf

⁶⁵ <http://stakeholders.ofcom.org.uk/binaries/enforcement/vod-services/Strictly-Broadband.pdf>

versions of their search results, which aim to exclude sexually explicit images and video. Paragraphs 3.17 and 3.19 include data on what technical method of control parents currently use.

4.14 Controlling illegal content and protecting minors from potentially harmful content are fundamental policy goals which require regulatory intervention, regardless of changes in technology and delivery of content.

4.15 The above findings highlight the importance of ensuring that any protection framework for online content should include a combination of the traditional standards protections and measures which provide the right framework for audiences to protect themselves and their families.

4.16 Convergence and the expanding consumption of connected devices will create further pressure on consumers' understanding of the regulatory environment, of the practices they can expect of service providers and of their awareness of their own responsibilities.

4.17 There is therefore a task for the Government, regulators and industry to ensure the provision of clear information, education and a framework of personal responsibility through which individuals and families can exercise an informed choice.

4.18 Industry will need to play a vital role in ensuring consumers are provided with clear information, education and a framework of tools and controls through which they can manage their own and their children's access to content. Such controls should be easy to use and find, and potentially available across all connected devices.

4.19 It is important to recognise, however, that the effectiveness and impact of online safety tools and content controls will depend on actions being taken by individuals and parents. Therefore, in order to ensure potentially harmful content is subject to comprehensive oversight, further consideration may be needed as to the roles and responsibilities of all industry players in the online environment.

SECTION 5

Preventing extremist and unlawful material

5.1 Ofcom has clear statutory duties to regulate extremist material on UK licensed broadcast services, including television channels delivered on the internet. We also have statutory powers to regulate such material for on-demand services notified in the UK. This section sets out some details of our experience of regulating this type of content, which may be useful for the Committee. Ofcom has no statutory powers to regulate extremist material on other online services.

Ofcom's experience of regulating television and radio broadcast services

Material intended to incite hate

5.2 Ofcom has statutory powers to set standards to protect audiences from harm from religious extremism broadcast on television and radio. Rule 3.1 of the Code states that "material likely to encourage or incite the commission of crime or lead to disorder must not be included in television or radio services". When considering potential breaches of Rule 3.1, a key factor that Ofcom takes into account is whether the content, as it was presented, contained a call to action which would be likely to encourage or incite the commission of crime or disorder.

5.3 Ofcom takes the issue of incitement to crime or violence extremely seriously. On the occasions where this issue has arisen, we have taken robust and appropriate action. For example, we have recently published four sanction decisions relating to the broadcast of material that was likely to encourage or incite the commission of crime (including hatred) and/or was abusive towards a religion or belief.⁶⁶

Unlawful content

5.4 If a broadcast service includes unlawful content, such as child abuse images, this would clearly be a matter for the criminal justice system. Ofcom would therefore report any such activity and the licensee responsible to the relevant authorities. Ofcom also has statutory powers to act quickly in response to the inclusion of any such content.

Ofcom's experience of co-regulation for on-demand content

Material intended to incite hate

5.5 Rule 10 in the ATVOD Rules reflects section 368E(1) of the Act and states that: "An on-demand programme service must not contain any material likely to incite hatred based on race, sex, religion or nationality".

⁶⁶ <http://stakeholders.ofcom.org.uk/binaries/enforcement/content-sanctions-adjudications/Rehmatul-DM-Digital.pdf>
<http://stakeholders.ofcom.org.uk/binaries/enforcement/content-sanctions-adjudications/regis1limited.pdf>
<http://stakeholders.ofcom.org.uk/binaries/enforcement/content-sanctions-adjudications/noor-tv.pdf>
<http://stakeholders.ofcom.org.uk/binaries/enforcement/content-sanctions-adjudications/takbeer.pdf>

5.6 To date there have been no cases where ATVOD has breached a notified ODPS under Rule 10.

Unlawful content

5.7 ATVOD's Rule 11 of the ATVOD Rules reflects section 368E(2) of the Communications Act and states that, "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."

5.8 ATVOD's Rule 11 captures content which is illegal, for example criminally obscene or indecent images. If content of this nature was included in a notified ODPS ATVOD would refer the service to Ofcom immediately. Ofcom would then immediately seek to suspend the service and notify the relevant authorities.

Ofcom's role for online content

5.9 Other than the regulatory duties we have set out above, which relate to television channels delivered on the internet and notified ODPS, Ofcom has no statutory powers to regulate hate material or abusive images online.

5.10 Illegal material such as child abuse images are within the remit of two bodies in the UK. The Internet Watch Foundation (IWF) is a self-regulatory regime funded by telecommunications and internet companies, which works to restrict the availability of child abuse images online; and the Child Exploitation and Online Protection Centre (CEOP), is the UK Police body dedicated to eradicating the sexual abuse of children. CEOP tracks and seeks prosecution of offenders, such as those who create, distribute or consume child abuse images. These bodies work closely together under a formal agreement.

5.11 Extremist material online is a substantial concern and poses significant risk to UK citizens. This will continue to be a clear regulatory challenge for the future. Industry-led approaches and tools will continue to play an important role in protecting audiences from such harmful content online.

SECTION 6

Preventing abusive comments on social media

6.1 Ofcom has experience of regulating abusive content on television and radio services, which may be of assistance to the Committee, details of which are set out below. While Ofcom has no statutory role to regulate abusive content, outside of television channels delivered on the internet, this section also sets out some research findings regarding children's behaviour and experience of online social media, which may be of both interest and use to the Committee.

Ofcom's experience of regulating television and radio broadcast services

6.2 Ofcom's Broadcasting Code contains rules which aim to protect audiences from abusive content on broadcast television and radio services. For example:

- Rule 3.1 of the Code states that "material likely to encourage or incite the commission of crime or lead to disorder must not be included in television or radio services";
- Rule 4.2 states that "the religious views and beliefs of those belonging to a particular religion or religious denomination must not be subject to abusive treatment";
- Rule 2.3 states that "in applying generally accepted standards broadcasters must ensure that material which may cause offence is justified by the context. Such material may include, but is not limited to...humiliation, distress, violation of human dignity, discriminatory treatment or language (for example on the grounds of age, disability, gender, race, religion, beliefs and sexual orientation)"; and
- Rule 7.1 states that "Broadcasters must avoid unjust or unfair treatment of individuals or organisations in programmes".

6.3 Ofcom recently sanctioned the licensee Takbeer TV Limited for serious breaches of Rule 4.1 "broadcasters must exercise the proper degree of responsibility with respect to the content of programmes which are religious programmes" and Rule 4.2 "the religious views and beliefs of those belonging to a particular religion or religious denomination must not be subject to abusive treatment". In this case the broadcast contained abusive statements about the Ahmadi Muslim community and beliefs.⁶⁷

6.4 In addition, Ofcom has recorded a series of breaches of Rule 4.2 of the Broadcasting Code against the licensee Ummah Channel Limited for broadcasting abusive content on its service, Ummah Channel. This television channel broadcast programmes which included terms and references when taken together amounted to "abusive treatment" of religious views and beliefs.⁶⁸

⁶⁷ <http://stakeholders.ofcom.org.uk/binaries/enforcement/content-sanctions-adjudications/takbeer.pdf>

⁶⁸ <http://stakeholders.ofcom.org.uk/binaries/enforcement/broadcast-bulletins/obb167/issue167.pdf>;
<http://stakeholders.ofcom.org.uk/binaries/enforcement/broadcast-bulletins/obb196/obb196.pdf>

Ofcom's experience of co-regulation for on-demand content

6.5 ATVOD has no rules to regulate abusive content on notified ODPS, ie content that is not considered to be hate speech or material likely to incite crime, or does not amount to R18 equivalent material.

Relevant research findings of online services

6.6 Our Media Literacy research into adults' and children/parents' media use and attitudes indicates that for the first time there is a decrease in the number of children with social networking profiles and there appears to be greater diversity in the types of social networking sites being used.

6.7 Other relevant findings include:

- Compared to 2012, children are less likely to know how to block messages from someone they don't want to hear from (53% vs. 68%) and to have done this in the past year (32% vs. 42%).
- 19% of 12–15s say they personally have had a negative experience, other than bullying, of online or mobile phone activity in the past year, where the most likely experience is gossip being spread (13%).
- Girls aged 12–15 are more likely than boys to have experienced gossip being spread about them online or through texts (17% vs. 10%) or to have seen/received something troubling online like a chain letter or something that makes them feel scared (4% vs. 0%).
- Girls aged 12–15 are more likely than boys to say they know of someone who has been bullied through a mobile phone (33% vs. 20%) and to say they have experienced bullying in this way (12% vs. 3%).
- Almost one in ten 12–15s and one in twenty-five 8–11s say they have experienced online bullying in the last year.
- Since 2012, those aged 12–15 with an active social networking profile are more likely to have a profile on Twitter (37% vs. 25% in 2012).

6.8 The above findings highlight further the importance of providing consumers with clear information, education and the right framework through which to protect themselves and their families from potentially harmful content of this kind.

6.9 As already stated, self-regulatory approaches will continue to play an important role in providing this framework in order to help protect adults and children in an online world. For example, there is increasing responsibility for industry to provide consumers with effective reporting tools, community standards or terms of use; and the need for transparent and demonstrably effective procedures for handling complaints and removing non-compliant content. It should be clear to consumers how to complain or what action to take if they see or hear content that is harmful or unsuitable for children.

6.10 The research findings also highlight the importance of providing children in particular with the right tools and media literacy skills to address this issue and understand the potential risks.

October 2013

Written evidence submitted by the Home Office

INTRODUCTION

1. This paper sets out the Home Office's evidence to the Culture, Media and Sport Committee inquiry into online safety.

2. Ensuring safety online, particularly for children, is a priority for Government. In a speech to the National Society for the Prevention of Cruelty to Children (NSPCC) the Prime Minister set out a range of measures to ensure that the cultural challenges of protecting children from accessing potentially harmful or age inappropriate content, and the challenges of restricting the availability of, and access to, criminal content such as child abuse material are met..

3. The Home Office's evidence focuses particularly on the Committee's concerns about illegal child abuse images online and illegal extremist materials online. It should be considered alongside evidence submitted by the Department for Culture, Media and Sport on harmful or age inappropriate content and threatening or abusive behaviour..

TACKLING ILLEGAL CHILD ABUSE IMAGES ONLINE

4. Research by the NSPCC indicates that about 5% of children in the UK suffer contact sexual abuse at some point during their childhood. Child abuse has many forms, one of which is online and multinational activity using sophisticated technology and techniques to evade law enforcement attention. The internet (including the so-called "hidden internet" which facilitates a sense of a "safe" community of offenders) is used

for the proliferation of indecent images of children. Work to tackle this between government, law enforcement and industry is an important part of the Organised Crime Strategy that was published on [7 October].

5. Images of child sexual abuse are illegal. It is illegal to take, make, circulate and distribute child abuse images (Protection of Children Act 1978)—such offences carry a maximum sentence of ten years’ imprisonment. It is illegal to possess indecent images of children (Criminal Justice Act 1988)—such offences carry a maximum sentence of five years’ imprisonment. Such offences apply equally online as they would offline.

6. The Government has worked with industry to develop some of the tightest controls in the world so that child abuse images are removed from the internet where possible, blocked from being accessed from the UK where they cannot be removed, and investigated so that those involved in their production, distribution or possession are brought to justice and so that the victims of these crimes can be protected and safeguarded. The Child exploitation and Online Protection Command of the National Crime Agency is central to this effort.

7. Tackling such abuse on the internet forms an important aspect of our wider approach to protecting children and vulnerable people—a key priority of this Government. The Government has established a Sexual Violence Against Children and Vulnerable People National Group (SVACV). This is a panel of experts and policy makers brought together by the Home Office to coordinate and implement the learning from recent inquiries into historic child sexual abuse and current sexual violence prevention issues. Tackling the misuse of the internet by those seeking to sexually abuse children, or gain personal gratification from it, is an important aspect of the National Group’s work. On 24 July 2013, the Government published a progress report and action plan on the work of the SVACV National Group. This contained clear activity already delivered by the Government to protect children online and an action plan to take forward further activity identified by the Group. The progress report and action plan can be found at the following link:

<https://www.gov.uk/government/publications/sexual-violence-against-children-and-vulnerable-people-national-group>.

REMOVING ILLEGAL CHILD ABUSE IMAGES FROM THE INTERNET AND PREVENTING ACCESS TO THEM

8. The Internet Watch Foundation (IWF) takes reports of illegal child abuse images from the public. It has the authority to hold and analyse these images through agreement with the Crown Prosecution Service and the Association of Chief Police Officers. The IWF assesses images, determines whether they are illegal and, if so, the severity of the images using Sentencing Council guidelines. Work is ongoing to expand the role of the IWF so that it can proactively search for child abuse images rather than being reliant on reports from industry and the public.

9. If the site hosting the image is located in the UK then the details will be passed to law enforcement agencies and the Internet Service Provider will be asked to take down the website using the “notice and takedown” process. In 2012, the Internet Watch Foundation found that 56% of UK child sexual abuse images were removed in 60 minutes or less from the point at which the Internet Service Provider or hosting provider was notified of the content. IWF Members remove 90% of such content within one hour, and 100% within two hours. In the past 17 years, over 400,000 webpages have been assessed—100,000 have been removed for containing criminal content. Less than 1% of child sexual abuse content is now thought to be hosted in the UK, down from 18% in 1996.

10. Where images are hosted outside the UK, the IWF will pass the details to their equivalent body in the country identified as hosting it so that they can take action. Often it is taken down completely, and the average time taken to remove child sexual abuse content hosted outside the UK had reduced to ten days in 2011 compared to over a month in 2008. Until the content is taken down the Internet Watch Foundation adds the URL to its “URL list” or “blocking list” which IWF Members can use to block access by their customers to the identified images. Such blocking arrangements currently apply to about 98.6% of domestic broadband lines.

11. The IWF is working with its members to introduce “splash pages”—these are warning messages that appear if a user attempts to access a webpage that has been removed for hosting illegal child abuse images, and they deliver a hard-hitting deterrence message to users seeking to access child abuse images.

12. These arrangements have been enormously successful, but the Government is committed to going further still in order to prevent offenders from being able to access child abuse images through the internet. That is why the Prime Minister, in his speech of 22 July, announced a further set of initiatives.

13. Internet search engine providers have been asked to go further in restricting access to illegal child sexual abuse images. They have been asked to do three things:

- (a) To work with law enforcement to develop effective deterrence messages to target those users who try to access child abuse images through their search engines.
- (b) To ensure that illegal child sexual abuse images are not returned in search results, and to use their search algorithms to guide users away from searches that could contain pathways to child abuse images.

- (c) To prevent any search results from being returned when specific search terms are used that have been identified by CEOP as being unambiguously aimed at accessing illegal child sexual abuse images.

14. The Government continues to work with search engine providers to put these measures in place. If progress is not forthcoming then the Government will consider bringing forward legislation to require their compliance.

15. The objective for all of these actions is to make it more difficult for unsophisticated users to find a route from open searching to more sophisticated offending environments, make it more difficult for inquisitive non-offenders to access indecent images of children, and make it less likely that members of the public could inadvertently come across such images.

INVESTIGATING THOSE RESPONSIBLE FOR ILLEGAL CHILD ABUSE IMAGES AND PROTECTING VICTIMS

16. The Child Exploitation and Online Protection Command of the National Crime Agency (CEOP) is the national lead for tackling sexual exploitation and sexual abuse of children. It is an integral part of the new National Crime Agency, that was established on 7 October 2013 to lead the UK's fight to cut serious and organised crime.

17. CEOP has done excellent work over the last seven years. It is dedicated to eradicating the sexual abuse of children, and supports both operational work to protect children and educational programmes to help children protect themselves online. It operates a reporting centre for children who want to report online sexual threats (in 2012–13 CEOP received an average of 1,600 reports per month of abuse from the public and the internet industry) a 14% increase on the previous year. This will have included direct reports from children. CEOP maintains close relationships with a wide range of stakeholders from law enforcement, industry and the educational sectors nationally and internationally. In 2012–13, CEOP safeguarded and protected 790 children, an increase of 85% on the previous year, and its work led to the arrest of 192 suspects. CEOP has now protected more than 2,250 children in its seven-year history.

18. Government funding for CEOP was higher in 2012/13 (£6.381m) than it was in 2009/10 (£6.353m). The CEOP budget has effectively been protected in cash terms since 2011/12 and there are now more people working in CEOP than at any time in its history.

19. Becoming a part of the NCA will bring advantages to CEOP. Its existing operating principles will be preserved as agreed when the Plan for the NCA was published, including its innovative partnerships with private and voluntary sectors. It will also gain access to more capacity to deal with complex cases of child sexual exploitation and abuse. It will gain greater resilience for front-line operational services and benefit from support from other NCA specialist functions such as the National Cyber Crime Unit. Its influence, as part of the national leadership the NCA will have across law enforcement, will be enhanced. The Crime and Courts Act 2013 places a statutory duty on the NCA to safeguard and promote the welfare of children in England and Wales, which means that all officers, not just those directly involved in child protection, will receive mandatory training on safeguarding children. This means that every one of over 4000 officers will have a legal duty to safeguard and promote child welfare so will be able to protect even more children from harm.

20. CEOP take the creation, distribution and accessing of illegal child sexual abuse images online extremely seriously. Not only do such images capture a child being sexually abused, but the viewing of such images can lead to an escalation in offending as well as continuing the victimisation of the child being abused in the image. A CEOP report in 2012 ("A Picture of Abuse") noted that research had identified a link between the possession of illegal images of children and the contact sexual abuse of children.

21. The Government will support CEOP and the police to tackle those involved in the creation, dissemination and accessing of child abuse images online. This includes ensuring that law enforcement agencies have the powers that they need to investigate offenders and bring them to justice, and to develop new capabilities that will enhance their effectiveness. The Prime Minister, in his speech of 22 July, announced plans for the creation of a new child abuse image database that would hold a national record of the images seized by the police. This would enable the police to identify known images more quickly on suspects' computers, will improve their ability to identify and safeguard victims from the images, and has the potential to enable industry to use the unique numerical "hash values" derived from the images to search for them on their networks and remove the before offenders can access them.

22. CEOP is also at the forefront of efforts to tackle more sophisticated offending where encryption and anonymisation is used by offenders to share illegal child abuse images through photo-sharing sites or networks away from the mainstream internet. This includes work in collaboration with the internet industry and the Internet Watch Foundation to tackle the peer-to-peer sharing of child abuse images.

WORKING TO TACKLE CHILD ABUSE IMAGES GLOBALLY:

23. In addition to the work of the IWF considered above, CEOP work extensively with their partners overseas to tackle the global threat from illegal child abuse images. CEOP participates in, leads and assists international investigations into illegal child sexual abuse images and online child sexual exploitation. CEOP is also a

founding member of the Virtual Global Taskforce which brings together law enforcement, public and third sector partners from across the world to tackle child abuse materials.

24. The UK strongly supports the work of the Global Alliance between the EU and US, with CEOP leading the work for the UK. The Deputy Director of CEOP is leading as the Driver on the EU EMPACT (European Multidisciplinary Platform against Criminal Threats) Cyber Child Sexual Exploitation initiative. The first meeting took place in October 2013 at Europol and agreed the Strategic Goals and Action Plan for 2014.

25. The Prime Minister has asked Joanna Shields, the Business Ambassador for Digital Industries, to lead industry engagement for a new UK—US taskforce to bring together the technical ability of the industry in both countries to tackle the use of the internet for child sexual abuse images. The Government expects to be able to make further announcements about the work of the taskforce in due course.

PREVENTION—HELPING CHILDREN PROTECT THEMSELVES AGAINST BECOMING VICTIMS

26. Online safety for children is of paramount importance to Government, and there are major cross-Government efforts taking place to ensure that children learn about staying safe online both in schools and through other initiatives.

27. CEOP's work to educate children and young people focuses particularly on the implications of their online behaviour, the "digital footprint" they leave, and the range of contact, content and conduct risks they face online. CEOP has developed a specific educational programme called ThinkuKnow to tackle this issue. The programme includes educational films and cartoons, teachers' packs and other online resources for use with children aged four—18. In 2012–13, over 2.6 million children saw the ThinkuKnow resources. In the same year, over 800 professionals in education, child protection and law enforcement have been trained by CEOP to educate children about online safety and how to respond to incidents. The Government, through CEOP, has now trained over 25,000 professionals who deliver these key messages to children in classrooms and other youth settings.

TACKLING MATERIAL INTENDED TO PROMOTE TERRORISM OR OTHER ACTS OF VIOLENCE ONLINE

28. Extremists use the internet to spread extremist messages to committed terrorists and those vulnerable to radicalisation. This material covers a spectrum from illegal Al Qaeda propaganda which incites violence like Inspire magazine, through to dedicated extremist forums and hate preacher videos on social media.

29. We know from recent attacks in Boston and Woolwich that online terrorist and extremist material remains one of a range of variables that can contribute to an individual becoming radicalised, and/or tipping into the acceptance of undertaking violent acts.⁶⁹ Our primary focus under the Prevent Strategy (2011) has therefore been to remove online material that breaches terrorism legislation. Proposals for going further to restrict access to this material will be discussed at the Extremism taskforce in October 2013.

CURRENT APPROACH—LIMITING ACCESS TO ILLEGAL/TERRORIST MATERIAL

30. A specialist police unit, the Counter Terrorism Referral Unit (CTIRU) currently take down material that breaches the Terrorism Act and is hosted in the UK, or—where we have strong relationships with industry. CTIRU proactively seeks to identify illegal material, and members of the public concerned about terrorist or extremist content online are able to refer material for investigation and potential removal by the CTIRU. In this respect, the CTIRU acts like the Internet Watch Foundation (IWF) in receiving reports and ensuring content is removed where possible.

31. Since it was established in 2010, CTIRU have taken down over 6000 pieces of material (more than 5,000 of which in the last 12 months). Even so, we would like to take down more terrorist content. However, a significant amount is hosted overseas and domestic law, even when it has extra-territorial jurisdiction, is of limited use. It would be difficult to prosecute a person or service provider operating outside the UK—they would have to be extradited to the UK to face prosecution and they could well argue that they had not engaged in criminal conduct in the country in which they were operating.

32. Where we cannot take down material, it is filtered from parts of the public estate (we have prioritised schools and some libraries). The filtering project has developed and our content list (of over 1000 URLs) is assessed by both CTIRU and the Crown Prosecution Service (CPS) to contain only URLs that are illegal. The main drawback with filtering is that UK users are still able to choose to view this illegal terrorist content (via desktop settings). We are considering how we can further restrict access to illegal terrorist material (potentially at the network level), further aligning with the IWF's approach.

33. There is no consistent global definition for what constitutes extremist material and the majority of harmful, offensive and inappropriate content online does not meet legal thresholds for action by law enforcement. For extremist material, this includes al-Awlaki's series of online sermons and practical instructions that can be of use to terrorists.

⁶⁹ Joint Terrorism Analysis Centre (JTAC) assessment 2013

IMPROVE THE INDUSTRY RESPONSE TO TERRORIST CONTENT

34. We aim to encourage the public and civil society groups to report legal but harmful content and seek to get it removed under industry terms and conditions. We are therefore working with industry to ensure their acceptable use policies are clear about what is tolerated on their platform and provide easy mechanisms to flag concerns about extreme content.

35. We are keen to see a consistently effective response to terrorist content across industry. We have seen some improvement following bilateral negotiations on individual acceptable use policies, but inconsistencies remain. Some companies run schemes which prioritise law enforcement referrals, however others make no explicit mention of terrorist or extremist content in their policies nor do they provide a single point of contact for law enforcement. Whilst engaging with industry to ensure that their own acceptable use policies are being applied rigorously, we are also considering the Home Affairs Select Committee recommendation of establishing a code of conduct for internet companies, distinct from their own terms and conditions, to improve the response to terrorist material (eg including “terrorism” as a category under unacceptable use).

36. We also tackle this problem from the user-end and run digital awareness projects that work with practitioners, parents and young people to ensure they have the skills to recognise and challenge extreme content. For example, through Prevent funding the Youth Justice Board have trained a hundred youth offending team practitioners to ensure they have skills to challenge and report extremism online and we have worked with Association of Chief Police Officers (ACPO) who have disseminated an internet safety DVD to local prevent projects, raising awareness of the issue. We will work with DCMS to ensure we are linked into initiatives such as Safer Internet Centre and Get Safe Online, which provide internet safety information and advice alongside a wealth of internet safety resources for schools and information for parents and children.

MAKING EXTREMIST CONTENT LESS ATTRACTIVE AND PROMOTING POSITIVE MESSAGES

37. We also seek to divert audiences and those vulnerable to radicalisation from extremist messages. The Research, Information and Communications Unit (RICU), part of the Office for Security and Counter Terrorism in the Home Office, aims to challenge and confront terrorist ideology and provide pathways for people to explore alternatives. Activity includes working with digital communications experts to help civil society groups make better use of the internet to counter extremist ideology. We intend to scale up this work.

38. RICU actively shares best practice on communications through the Global Counter Terrorism Forum, the EU Radicalisation Awareness Network, and in bilateral work with the US and other countries.

October 2013

Written evidence submitted by the Department for Culture, Media and Sport

1. INTRODUCTION

1. The Government welcomes this inquiry into online safety. The internet has transformed our lives; changing the way we interact with one another, promoting the development of new and innovative technologies and driving the UK’s economic ambitions for the future. The UK has built strong digital foundations, and is reaping the benefits—it is estimated that in 2010 the digital economy accounted for over 8% of GDP, a greater proportion than in any other G20 country.⁷⁰

2. Government’s aim is for the UK to be a nation of confident and safe consumers, able to make the most of the opportunities the digital world has to offer. However, in the face of such rapid technological and cultural change—as well as maximising the benefits the internet brings—we must be aware of, and responsive to, the risks it presents. In July this year, Government published a policy paper, “Connectivity, content and consumers: Britain’s digital platform for growth”⁷¹ following its review of the media and telecommunications sectors. This policy paper considers the issue of online safety but also sites it in the context of the wider media environment.

3. Ensuring safety online, particularly for children, is a priority for Government. In a speech⁷² on 22 July to the National Society for the Prevention of Cruelty to Children (NSPCC) the Prime Minister set out a range of measures to ensure that the cultural challenges of protecting children from accessing potentially harmful or age inappropriate content, and the challenges of restricting the availability of, and access to, criminal content such as child abuse material are met. This evidence considers harmful or age inappropriate content (section 2) and threatening or abusive behaviour (section 3). The Home Office will be submitting written evidence in relation to illegal content separately.

⁷⁰ Boston Consulting Group

⁷¹ <https://www.gov.uk/government/publications/connectivity-content-and-consumers-britains-digital-platform-for-growth>

⁷² <https://www.gov.uk/government/speeches/the-internet-and-pornography-prime-minister-calls-for-action>

2. HARMFUL CONTENT

4. Currently, 91% of children live in households with internet access and a greater proportion of children aged 12–15 own smartphones than adults.⁷³ While consenting adults should be free to watch the legal content they choose, and while children and young people are important consumers of digital content, it is the case children's use of the internet can be a cause of concern for parents. Government understands that, first and foremost, responsibility for keeping children safe online falls to parents and guardians; however, Government is acting to ensure that parents have the tools and information they need to be able to do so.

UK Council on Child Internet Safety (UKCCIS)

5. Government believes that a multi-stakeholder approach to the issue of limiting the access of children to harmful content is the most effective way to deliver results. The Government has been working through the UK Council for Child Internet Safety (UKCCIS), which brings together more than 200 organisations across the information and communication industries, law enforcement, regulators, academia, and charities—to pursue a voluntary approach to child internet safety and has called on industry to make the right tools available to allow parents to protect children online.

Measures for limiting access to harmful content

6. In his speech on 22 July, the Prime Minister outlined the range of measures Government is working with industry to deliver which will help parents and guardians limit children's access to harmful or age inappropriate content:

- *Domestic internet filtering*: Providing parents and guardians with easy-to-use and effective tools to help limit the content that children can access in the home is a key aspect of the overall package of measures that should be available. Government has been working with industry to secure the commitment that, by the end of this year, the four largest internet service providers (ISPs)—BT, Virgin Media, Sky and TalkTalk making up almost 90% of the fixed broadband market⁷⁴—will provide, free of charge, family-friendly network-level filtering (covering all of the devices in the home which connect to that internet service) for *new customers* by the end of this year. This will mean that, when someone sets up a new broadband account, the settings to install family-friendly filters will be automatically selected; if customers just click next or enter, then the filters would automatically be on. ISPs have also committed to contacting *existing customers* through 2014 and providing them with an unavoidable choice on whether or not to set up filters. Again, this will be free of charge. While the technology being deployed by each of the ISPs is different, based on the differing infrastructure they have in place, the family-friendly filtering solutions offered will include a number of customisable options, allowing parents to select or de-select categories of content, “black-list” or “white-list” (filter or ensure access, respectively) certain URLs, dependent upon their own specific circumstances.
- *Verification of those setting the filters*: ISPs have also committed to developing processes to ensure that the person setting the filters are aged 18 or over, so avoiding the situation that it is a child setting the filtering levels. It is anticipated that this will be delivered through a “closed-loop” email system where the main account holder will be contacted to verify the setting of filters, and informed if the settings on the filters are changed subsequently.
- *Smaller ISPs*: While the largest ISPs cover almost 90% of the broadband market, Government is exploring options for the smaller ISPs—through the Internet Service Providers' Association (ISPA)—to deliver tools and solutions to their domestic consumers which can put users in control of the content they, and their family, receive.
- *Filtered public Wi-Fi*: The six largest wireless internet providers (Arqiva, BT, Nomad, Sky, Virgin and O2) covering around 90% of the market committed to, and have implemented, publicly available family-friendly Wi-Fi in places where children regularly visit, ensuring that children are unable to access pornographic content.
- *Mobile phone filtering*: The Mobile Broadband Group published a UK “Code of Practice for new forms of Content on Mobile” in 2005 which requires mobile network operators (MNOs) to provide a filter to their internet access services. Whilst the vast majority of providers are filtering internet services in this way, coupled with robust age verification processes, Three—as the last major operator to fully implement these measures—has committed to doing so.
- *Public awareness campaign*: The largest ISPs are working to develop an awareness campaign for parents for next year. This campaign will provide support and advice to parents about bringing their parenting skills into the online world and will complement plans by Government to highlight internet safety messages in interactions it has with citizens.

⁷³ Source: Ofcom Children and Parents: Media Use and Attitudes Report Oct 2012— <http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/oct2012/main.pdf>

⁷⁴ Source: Ofcom Communications Market Report 2013 http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr13/2013_UK_CMR.pdf

- *Ofcom reporting*: Ofcom has been asked to report, by the end of this year, on a number of areas in relation to child internet safety—predominantly around parental awareness of, and confidence in using, the internet safety tools available. A further report, in a year's time, will help assess whether levels of parental awareness and confidence have increased as a result of these measures.

7. While these will provide a range of tools to help support parents and guardians to make sure children do not access harmful or age inappropriate content Government is clear that technology is not the only way in which this issue should be addressed. Ensuring that children are resilient, competent and confident when online is important and education is a key aspect of this.

Education

8. As part of the government's reforms to the *national curriculum*, it will be strengthening the requirements to teach e-safety as part of changes to the new computing programmes of study. The existing national curriculum only requires e-safety to be taught to 11 to 16 year olds in key stages 3 and 4. From September 2014 e-safety will be taught to pupils at all key stages, from primary pupils aged five through to secondary pupils aged 16.

9. There is also the award-winning programme for children and parents *Think U Know*⁷⁵ which is produced by the Child Exploitation and Online Protection Centre (CEOP—part of the Serious Organised Crime Agency, a Government Agency). Through trained volunteers, this programme reaches hundreds of thousands of children each year, educating them on topics such as grooming and sexting. CEOP falls under the command of the National Crime Agency on 7 October.

10. The UK's *Safer Internet Centre*⁷⁶ (supported with EU funds) has a hotline for internet safety information and advice and provides a wealth of internet safety resources for schools and information for parents and children. The Centre leads on activity for Safer Internet Day in February each year which attracts significant media coverage (this year on BBC Radio 1 and 5 Live in addition to coverage on Facebook and Google).

11. *Get Safe Online*⁷⁷ is a joint initiative between the Government, law enforcement, leading businesses and the public sector. Their aim is to provide computer users and small businesses with free, independent, user-friendly advice that will allow them to use the internet confidently, safely and securely. Working with Get Safe Online, the National Fraud Authority's e-Confidence campaign begins in October.

12. Childnet is a children's charity working in the area of policy and has developed a range of award-winning websites and resources to help provide children, parents and teachers with the information and skills they need to use the internet safely and responsibly. Examples of Childnet's work include the *Know IT All*⁷⁸ suite of resources, the guidance for schools on cyberbullying, the Let's Fight it together film, and many more.

13. The *South West Grid for Learning*⁷⁹ is a not for profit, charitable trust company, that specialises in supporting organisations with online safety. It was established in 2000 to provide schools and many other educational establishments throughout the South West of England with safe broadband internet connectivity; broadband-enabled learning resources but especially providing professionals, parents and children with advice, resources and support in using the internet safely across the wider UK.

14. *ParentPort*⁸⁰ was launched in October 2011, following the Bailey Review, to make it easier for parents to complain about material they see or hear across the media, communications and retail industries. ParentPort is run by the UK's media regulators and provides parents with useful information about media standards and internet safety as well as giving parents an easy way to make a complaint and share their views with the regulators.

3. ABUSIVE OR THREATENING BEHAVIOUR

15. The issue of abusive or threatening behaviour—whether targeted at adults or children—over the internet is an area of concern for Government. However, the legislative position in relation to this is clear; where behaviour is illegal off-line it is also illegal on-line and there are a number of pieces of legislation which can be, and are, used to prosecute.

Legislation and Director of Public Prosecutions (DPP) Guidance

16. Communications sent via social media are capable of amounting to criminal offences in relation to a range of legislation. Including:

- Communications which may constitute *credible threats* of violence to the person or damage to property.

⁷⁵ <http://www.thinkuknow.co.uk/>

⁷⁶ <http://www.saferinternet.org.uk/>

⁷⁷ <https://www.getsafeonline.org/>

⁷⁸ <http://www.childnet.com/resources/kia/>

⁷⁹ <http://www.swgfl.org.uk/Staying-Safe>

⁸⁰ <http://www.parentport.org.uk/>

- Communications which *specifically target an individual or individuals* and which may constitute harassment or stalking within the meaning of the Protection from Harassment Act 1997.
- Communications which may be considered *grossly offensive, indecent, obscene or false*.

17. Communications which are grossly offence, obscene, indecent or false fall to be considered either under section 1 of the Malicious Communications Act 1988 or under section 127 of the Communications Act 2003.

18. Section 1 of the Malicious Communications Act 1988 makes it an offence to send to another person:

- (a) an electronic communication which conveys:
 - (i) a message which is indecent or grossly offensive;
 - (ii) a threat; or
 - (iii) information which is false, and is known or believed to be false by the sender; or
- (b) any electronic communication which is, in whole or part, of an indecent or grossly offensive nature, provided that one of the purposes of sending the communication is to cause distress or anxiety to the recipient. The offence is one of sending, delivering or transmitting, so there is no legal requirement for the communication to reach the intended recipient.

19. Section 127 of the *Communications Act 2003* makes it an offence to send or cause to be sent through a “public electronic communications network” a message or other matter that is “grossly offensive” or of an “indecent, obscene or menacing character”. The same section also provides that it is an offence to send or cause to be sent a message that the person knows to be false “for the purpose of causing annoyance, inconvenience or needless anxiety to another”. The defendant must be shown to have intended or be aware that the message was grossly offensive, indecent or menacing, which can be inferred from the terms of the message or from the defendant’s knowledge of the likely recipient. The offence is committed by sending the message. There is no requirement that any person sees the message or be offended by it.

20. Other relevant legislation includes:

- Offences Against the Person Act 1861;
- Computer Misuse Act 1990;
- Protection from Harassment Act 1997;
- The Criminal Justice and Public Order Act 1994; and
- Section 15 Sexual Offences Act 2003 (for grooming)

21. In June 2013, following consultation, the *Director for Public Prosecutions published guidelines*⁸¹ for prosecutors when considering cases involving communications sent via social media. These guidelines set out that prosecutors (subject to general guidelines around having sufficient evidence and whether prosecution is in the public interest) should, when considering whether communications sent via social media are capable of amounting to criminal offences, make an initial assessment of the content of the communications and the conduct to distinguish between:

- There is a credible threat of violence.
- Where communications specifically target an individual or individuals.
- Where communications breach a court order.
- Where communications may be considered grossly offensive, indecent, obscene or false.

22. These guidelines seek to draw the difficult balance between protecting freedom of speech on the one hand with acting robustly against communications which cross the threshold into illegality.

23. Data from the Crime Survey for England and Wales (below) shows that whilst almost a third of adults had some form of negative experience online, the majority were related to viruses. The proportions of people experiencing “upsetting/illegal images” and “threatening/abusive behaviour” are much lower, and some of those experiences are also likely not to have met the criminal threshold.

<i>Experience of negative incidents online among adults aged 16 and over</i>		
	<i>2010–11</i>	<i>2011–12</i>
Computer virus	26.0%	24.6%
Loss of money	2.6%	2.6%
Unauthorised access to/use of personal data	4.5%	5.2%
Upsetting/illegal images	3.1%	3.5%
Abusive/threatening behaviour	1.6%	1.4%
Any of the above incidents	30.5%	29.4%
Other (ie experienced no incident)	69.5%	70.6%

⁸¹ http://www.cps.gov.uk/news/latest_news/dpp_publishes_final_guidelines_for_prosecutions_involving_social_media_communications/

Acceptable use policies and reporting mechanisms

24. In the vast majority of cases communications sent via social media will not cross the threshold into criminal behaviour but may still cause offence to other users. Where this is the case, Government expects social media companies, and others, to have robust processes in place promptly when abuse is reported; including acting expeditiously to assess the report, removing content which does not comply with the acceptable use policies or terms and conditions in place and, where appropriate, suspending or terminating the accounts of those breaching the rules in place.

25. A UKCCIS working group has been looking at the issue of transparency of reporting processes following reports of abuse by social network users and difficulties with complaints and reporting. Parents and children have indicated that they often cannot easily make a report, that their report may not be handled quickly and they are given little feedback about how their reports are dealt with. Ministers will consider how this work can best be taken forward at the next UKCCIS board meeting on 6 November.

October 2013

Supplementary written evidence submitted by the NSPCC

INTRODUCTION

1. The NSPCC welcomed the opportunity to respond to the Culture, Media and Sport (CMS) Select Committee inquiry into online safety in September, and we were delighted to be invited to come before the committee in October to give oral evidence.

2. Since then, the NSPCC has released further research on the issue of online safety and was the only children's charity to be involved in the Prime Minister's internet safety summit in November. As such, we have requested to submit supplementary evidence to the inquiry, to be read alongside our original response. We hope both the statistics and perspectives included here are helpful for the Committee when making its recommendations.

HARMFUL CONTACT ONLINE

NEW KEY STATS

- **10,600** young people contacted ChildLine in 2012–13 for support and advice on how to deal with internet safety related issues—a **65% increase** on the year before⁸²
- **4,507** young people contacted ChildLine in 2012–13 for support and advice on how to deal with being bullied online—an **87% increase** on the year before⁸³
- More than **One in Four** 11–16 year olds with a social networking profile have experienced something upsetting on a social networking site.⁸⁴

3. Research the NSPCC is about to launch research which shows that **28%** of young people who have a social networking profile have experienced something that has upset them in the last year. These experiences include cyberstalking, being subjected to aggressive or offensive language, being sent sexually explicit pictures and being asked to provide personal or private information. However, the greatest proportion of this group (**37%**) told us that they had experienced “trolling”. Another alarming statistic showed that **over half** of these young people said they did not know the person who was responsible for the behaviour that upset them.

4. Alongside this evidence that online bullying is clearly a problem for young people in the UK, the latest ChildLine statistics showed an **87% increase** in 2012–13 in the number of young people contacting us to ask for support and advice about being bullied via social networking sites, chat rooms, online gaming sites, or via their mobile phones. We believe the increasing ownership of smartphones and tablets by young people is likely to be contributing to this trend.

5. In our original submission to the Committee the NSPCC described the need for online safety, including information about respectful behaviours and managing upsetting experiences, to be a core part of the national curriculum, taught through compulsory Sex and Relationships Education (SRE). We also called for social networking sites and other technological leaders to provide straightforward and meaningful ways to report abuse online. We continue to call for this action and in addition the NSPCC would be delighted if the Committee could support the following asks:

- *The UK Council for Child Internet Safety (UKCCIS)* Executive Board should make tackling the risks children experience on social networking sites a priority
- *Ofcom*—should play a greater role in providing easily accessible information to parents about social networking sites

⁸² *Can I tell you something?*, ChildLine Review 2012/13 (Jan 2014) http://www.nspcc.org.uk/news-and-views/media-centre/press-releases/2014/childline-report/childline-report_can-i-tell-you-something_wdf100354.pdf

⁸³ Ibid

⁸⁴ New NSPCC research due for release end Feb 2014

- *Social networking sites and others*—should offer a range of options for how to report illegal or offensive bullying or content and default privacy settings should be set to the highest levels possible for users under 18. The NSPCC also believes sites should provide incentives for new users to take safety and etiquette tutorials.

6. Additional to the issue of online bullying, the ChildLine annual review, *Can I tell you something?* also showed that **1061** young people specifically talked about online sexual abuse, with girls being the most affected. ChildLine also saw a **28% increase** in contacts from young people who talked about being asked to post sexually provocative images online, or share them via a mobile phone.

7. The NSPCC remains adamant that children should be given strategies to resist unwanted sexual approaches, encouraged to report upsetting experiences online and be taught about online safety as part of compulsory SRE lessons at school. We are pleased that the Government has committed to emailing out to every school SRE advice developed by Brook, the Sex Education Forum and others. This is a helpful interim measure to address the current shortfall in up-to-date statutory SRE guidance. However, we believe the Government should commit to updating the official SRE guidance from 2000 to include issues children face in today's world, like staying safe online.

8. We do, of course, believe parents have a central role in talking to their children about how to stay safe online. We appreciate these conversations might feel daunting, but we believe parents needn't be experts on the internet, but instead treat online safety as they would any other form of parenting where rules and boundaries need to be set.

9. We also recognise that other agencies that work with children and prioritise children's safety should play a role alongside schools and parents in providing online safety advice and education. The NSPCC in October 2013 launched the ChildLine ZipIt app to discourage children from sending sexually explicit messages. This has already been downloaded by 40,000 young people so far. We have also developed in collaboration with CEOP the *Keeping Children Safe Online* e-learning course aimed at any organisation or professional working with children.

AGE-INAPPROPRIATE CONTENT

NEW KEY STATS

- **63%** of children aged 11–12, who use a social networking site, have a profile on Facebook, and **28%** use Twitter despite the minimum age for registration on both sites being set at 13.⁸⁵
- **28%** of over 601 school pupils surveyed by the NSPCC think pornography definitely “influences how young people have to behave in a relationship.”⁸⁶

10. Based on our research, we estimate that half of all the 11 and 12 year olds in the UK use services that have a minimum age of 13. The NSPCC is concerned that this leaves them vulnerable to engaging with content and behaviours that are not appropriate for their age. In addition, ChildLine counselled 475 young people who had been exposed to sexually explicit images or internet pornography and almost one third of children surveyed by the NSPCC about watching pornography said it affected the way they acted when they were in a relationship.

11. We support plans by the major Internet Service Providers (ISP) to launch a national campaign to help parents use the filters and tools that are available to them to manage the online content to which their children have access, and more broadly help parents to understand more about internet safety. To support these efforts, the NSPCC also calls for:

- *UKCCIS*—to undertake a robust and independent evaluation of the ISPs campaign to measure its effectiveness and push for improvements where needed
- *The Government*—should evaluate the effectiveness of active choice plus and be prepared to explore legislative solutions to children accessing adult content and services.

CHILD ABUSE IMAGES

12. In our original evidence to the Committee the NSPCC explained that a Freedom of Information request we made in 2010 revealed that nearly 26 million child sexual abuse images had been confiscated in the preceding two years from just five of the 43 police forces in England and Wales which were able to check their records. At that time most forces said it would take too long to interrogate files to see how many pictures of children being sexually abused they had accumulated during investigations. However, estimates of the number of online child abuse images confiscated by police in England and Wales each year in the UK range from 100–360 million.⁸⁷

⁸⁵ NSPCC, *Younger Children and Social Networking Sites: A Blind Spot?* (Nov 2013) http://www.nspcc.org.uk/Inform/resourcesforprofessionals/online-safety/younger-children-report_wdf99929.pdf

⁸⁶ NSPCC (Sept 2013) http://www.nspcc.org.uk/news-and-views/our-news/child-protection-news/telegraph-better-sex-education/online-porn-dictates-young-people-relationships_wda98264.html

⁸⁷ NSPCC (Oct 2012) http://www.nspcc.org.uk/news-and-views/media-centre/press-releases/2012/12-10-15-urgent-action-child-abuse-images/urgent-action-child-abuse-images_wdn92344.html

13. The NSPCC welcomed the opportunity to contribute to the Prime Minister's internet safety summit in November, and we were pleased by the commitment shown by the leading search engines to ensure that tens of thousands of the most disturbing search terms will return only "clean" results and warnings about child abuse imagery. We now urge the Government and industry to work together to monitor and evaluate the effectiveness of these technological solutions and make improvements where needed.

14. Alongside this proactive approach from industry, we want to see a tireless commitment to policing efforts to tackle child abuse images from the CEOP command within the new National Crime Agency. Images of child abuse was mentioned briefly in the NCA's 2013–14 Annual Plan as an operational priority:

*"To tackle the enablers of crime that have both utility and impact across several threat areas. For example cyber-enabled criminality where access to the hidden internet can facilitate criminal acts such as illicit drugs supply, images of child abuse and the trade in stolen credit card data."*⁸⁸

15. However, we hope that the Agency's programme of work on child abuse images will feature much more extensively in its next annual plan, and more broadly on policing the NSPCC wants to see:

- A greater number of arrests and prosecutions for offences relating to child abuse images.
- A commitment to identifying and destabilising the criminals at the centre of child abuse image networks.
- A greater focus on tackling child abuse images at a local level from Police and Crime Commissioners, and in Police and Crime Plans.

16. The NSPCC also eagerly awaits the work of the UK/US taskforce on child abuse images which we hope will encourage action from the internet and technology industries to apply their technical expertise to develop innovative solutions to this global challenge.

January 2014

⁸⁸ National Crime Agency Annual Plan 2013/14 (Oct 2013), p.7 <http://www.nationalcrimeagency.gov.uk/publications/33-nca-annual-plan-2013-14/file>