children's charities' coalition on internet safety

Mr John Whittingdale MP, OBE
Chairman, DCMS Select Committee
House of Commons, London SW1A 0AA
30th September, 2013

Dear Mr Whittingdale,

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.

Yours sincerely,
John Carr OBE
Secretary, Children's Charities' Coalition on Internet Safety
10, Great Queen Street, London WC2B 5DD
chisgb@outook.com
www.chis.org.uk

- **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 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 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 e.g. 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 e.g. 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 e.g. 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 identify 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.

---ooo---