Department for Education consultation on parental controls.

Open Rights Group response. September 2012.

For more information please contact Peter Bradwell, peter@openrightsgroup.org

Key points and summary

- The Government should not mandate network level filtering. If they do, they will be constructing an infrastructure of censorship that will be inefficient, prone to errors and open to abuse.
- Default internet filtering ultimately moves decisions about what is appropriate for families and households further out of parents' hands. The Government should promote an 'active choice' model that encourages parents to make their own decisions about what is appropriate and what tools to use.
- Mandating network level filtering would amount to a significant market intervention that would disrupt an emerging market for Internet access tools, whilst imposing significant costs on Internet Service Providers. We see no evidence of overwhelming public support for default network level filtering[1].
- The available evidence does not support moves to implement a default 'on' Internet filter, and suggests that technical measures such as filtering are not effective as a means to prevent children's exposure to risk online[2]. Filters can also give parents a false sense of security, with engaged parenting shown to be more effective.
- Filtering systems often, through error, overreach or abuse, lead to the blocking of legal and legitimate content.
- The Government should work with industry and parents to make sure clear and easy to understand guidance, advice and tools are available, including information about the best ways to manage children's internet access and what tools are available.

We welcome the opportunity to respond to this consultation and the attention the Department for Education are affording internet safety and child protection. We have responded to some of the questions in the consultation response form below, with this introduction designed to summarise our key points and draw attention to some of the broader issues about Internet filtering.

We agree that protecting children from the diverse risks they face online is a crucial issue that requires action from parents, businesses and government. However, we do not believe that default-on network level filtering is the best way to achieve the goal of protecting children online. Parents should be supported in making their own decisions about what tools are appropriate for their family. A healthy market for parental controls is developing; everything proposed regarding filtering technology is available to parents already. The Government's role should be to support this by working with industry to ensure these are easily available and that parents understand how to use them.

We appreciate the Department seeking the views of parents on this matter via the consultation form, and the questions aimed at some technology companies. However, we suggest that the consultation response form discourages evidence about broader issues such as the full range of evidence about the risks online for children and the relative merits of different ways of addressing these risks.

[1] We are aware of a petition from the Safety Net campaign. However, as discussed below, wider and more representative surveys suggest public support for an active choice approach.

[2] See http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20III/Reports/ParentalMediation.pdf

Due to the narrow set of questions in the consultation form, we recommend that the sample of responses gathered through this consultation should be seen as part of a wider field of evidence. For example, this should include an analysis of the merits and problems with the variety of access restriction tools and a look at the evidence of parental attitudes and from studies such as the EU Kids Online project[3]. To give this work coherence, the Government needs to take a clear position on what they are trying to achieve by intervening on this issue.

Our response to this consultation draws on our research into mobile Internet filtering, which in most cases is already turned on by default on mobile phone accounts. We have submitted a copy of this report along with our response to the consultation. In the report[4], which was jointly published with LSE Media Policy Project earlier this year, we show how content that could not be considered 'adult' is being blocked by mobile networks. The worthwhile aspiration to help parents manage their children's Internet access has led to filtering systems that are clumsy, inaccurate, and inefficient, based on opaque and error-ridden lists of sites considered 'blockable'.

What is at stake

The decision to implement filtering is about the power to decide what people can see and do online. Technology has put the ability to share information and organise and create new services into people's own hands. This is the beating heart of the Internet and lies behind its potential as a driver of social and economic innovation. Network level filtering systems take back that power from people and place decisions about access to information under the control of the Government, the technology industry and over-broad and unresponsive filtering systems.

Where filtering is mandatory – meaning imposed by the Government or mandated by a court order with no choice to have filtering applied – questions about necessity, proportionality, and due legal process become even more significant. The consequences of mobile filtering already help to demonstrate that seemingly simple, laudable goals such as protecting children through technical intervention may have significant harmful and unintended consequences for everybody's access to information.

We note in this context that the UK has repeatedly made commitments to freedom of expression and privacy on the Internet, aimed both at the UK and internationally. In December 2011, Foreign Secretary William Hague noted the importance of these rights, and the UK Government's commitment to them, in his remarks at the London Conference on Cyberspace[5]. In a letter to freedom of expression advocates shortly afterwards, he then noted the preference for active choice in the context of child protection in the UK:

> *"Active choice is the preferred approach...It is important to distinguish between government encouraging people to make more use of existing protections as a matter of choice, and the government deciding what people can and cannot do online. Our plans do not prevent access to legal material, but seek to make it much clearer that protections exist, and to encourage their use. The position of Claire Perry regarding the default filtering of adult content is not the position of this government."*[6]

Where the Government mandates network level filtering, there will, through mistakes, abuse or overreach, be restrictions on access to legal and legitimate material. Where anything other than

[3] See for example http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/EUKidsOnlineIIReports/Final%20report.pdf

[4] See http://www.openrightsgroup.org/ourwork/reports/mobile-internet-censorship:-whats-happening-and-what-we-can-do-about-it

[5] See http://www.fco.gov.uk/en/news/latest-news/?view=Speech&id=685672482

[6] The Foreign Secretary's reply on UK Internet freedom, Open Rights Group blog, January 05, 2012

active choice is mandated, the government and industry will be making assumptions about what is best for a family which cannot possibly reflect the diversity of needs and attitudes of the UK's parents and their children.

Active choice

We would also note the studies conducted for the Government into this issue over the past few years – the Byron Review (and follow up report) and the more recent Bailey Review. In particular we note their support for active choice, and their conclusions about the importance of active parenting and concerns they set out about any reliance on filtering technologies.

In October 2011, four major ISPs signed up to a voluntary code of practice that outlined a commitment to roll-out active choice over the year to October 2012. This set a useful timetable with clear actions for those in the industry to pursue. It is unclear why this code has not been given time to work, after which the government could have assessed its impact and effectiveness.

We also recommend that the Government is clearer about what it is trying to achieve, and whether the aim is to reduce children's access to pornography, to reduce the availability and address the impact of pornography in general, or to address the broad issue of the risks that children and young people face online. These different issues require different analyses and responses and conflating them is not helpful.

We suggest a proportionate focus that takes into account the many opportunities and challenges the Internet presents to children and young people, and recommend that the Government closely analyses the evidence about the extent of children and young people's exposure to risk and harmful or undesirable content online.

We recommend that the government maintains their existing commitment to a policy of active choice (rather than modified active choice suggested in question 10c), concentrating on users and devices rather than networks and on helping parents make informed decisions about what tools to use to manage their children's access to the Internet. The government should avoid mandating the use of network filtering and support an 'active choice' with no default options selected.

Responses to consultation questions

Q6: On the responsibilities of parents and businesses

Making sure children and young people are safe online and are capable of dealing with risk is primarily a parental responsibility, but one that is shared with businesses, government, civil society and children and young people themselves.

It would be odd to suggest that one group in this complex social issue has sole responsibility. Instead of asking whether businesses or parents have responsibility, the better question would be: what responsibilities does each party have?

We would argue that industry has a responsibility to provide educational and technical resources that parents can use in the home to help manage the risks associated with access to the Internet.

For example, we note that Vodafone's magazine 'Digital Parenting' and resource site for parents provides useful information and guidance on child safety online[7]. This is preferable to an approach from an ISP that simply offers a filtering service which may encourage parents to consider that the issue of child safety is taken care of.

ISPs should also ensure that there is a simple and easy way to communicate with them about parental controls, consistent with paragraph 4.6 of the October 2011 Code of Practice. This should help allay fears set out by Helen Goodman MP, in the evidence session of the Premier Christian Media sponsored review of online child protection, that it may be difficult to communicate with ISPs about filtering software[8].

Parents have a responsibility to understand the issues associated with inappropriate content, contact and conduct. Only one of these can be addressed, even marginally, through filtering.

Children themselves also share this responsibility. When considering the best way for young people and their parents to deal with online risks, including exposure to undesirable content, a Europe-wide study led by Professor Sonia Livingstone concluded that children should be helped to 'self-regulate'. Industry should complement these efforts by helping parents use tools to filter and monitor their children's use:

> *'It is important...to encourage children to be responsible for their own safety as much as possible rather than rely on restrictive or adult forms of mediation'*[9]

This is consistent with the conclusions Professor Tanya Byron reached in the reviews she carried out for the UK government in 2008 and 2010 of the risks that children face from the Internet and video games. Byron emphasised the need for a mix of filtering tools and parental engagement, arguing that to place too much emphasis on the former could lull some parents into a false sense of security[10].

The Government has a responsibility to understand the issues and provide national coordination for education and public awareness, and ensure that parents have the information and tools available to them.

[7] http://parents.vodafone.com/

[8] See http://www.claireperry.org.uk/downloads/independent-parliamentary-inquiry-into-online-child-protection.pdf page 87

[9] Livingstone, S., Haddon, L., Görzig, A., and Ólafsson, K. (2011). Risks and safety on the internet: The perspective of European children. Full Findings. LSE, London: EU Kids Online

[10] See "Safer Children in a Digital World: The Report of the Byron Review", 2008 and "Do we have safer children in a digital world? A review of progress since the 2008 Byron Review", 2010

Q7: Which of the following types of internet content and online behaviour do you know for sure that your children have been exposed to?

Q8: "Which types of internet content and online behaviour do you think most worries your children?"

Q9: "Which of these issues listed in Questions 7 and 8, do you think you need most help protecting your children from online?"

We welcome the soliciting of parents' opinion on these questions. We recommend that the results are considered in the context of other work on children's and parents' knowledge and attitudes, such as the work by Professor Sonia Livingstone already noted.

This is an emotive issue and responses to it need to be guided by robust evidence. It is possible to allow the strength of emotion felt towards a particular goal – for example protecting children online – to inhibit a proper analysis of how to achieve it. This is not a decision about *whether* the Government thinks it is important to protect children online. It is about the best way of doing so. Understanding the nature of the issue therefore requires clear and reliable evidence.

There is likely a diverse range of content that parents are concerned their children can access. This is unlikely to be just an adult content issue, with different parents considering different interventions appropriate. For example, TalkTalk suggested that early findings from the use of their filtering system showed parents were most concerned with sites associated with self-harm and suicide[11]. By working with ISPs to look at their experiences with parents, the Government will likely gain a helpful further indication of parents' needs.

When looking at young people's experiences of risk online, the team of researchers working on the 'EU Kids Online' study led by Professor Livingstone found that, "One quarter of UK 9-16 year olds say that they have seen sexual images in the past 12 months, whether online or offline. However...11% encountered sexual images online."

They concluded that, 'Overall, most children have not experienced sexual images online and, even of those who have, most say they were not bothered or upset by them'. Of those who said they had seen sexual images online, 24%, or 3% of all the children surveyed, claimed they were upset or bothered by something they had seen[12].

We are concerned at some of the statistics and evidence cited by the Safety Net campaign, which advocates default on filtering. For example, 'facts' regarding young people's exposure to adult material, including the claim that '1 in 3 10 year olds have seen pornography online' are based on a discussion that Psychologies magazine had with an unknown number of 14-16 year old boys at one school. The statistics in that article are accompanied by an article that features no citations for the factual assertions about the scale of young people's access to adult or harmful material.

In a report on their findings, the researchers for the EU Kids Online study led by Professor Livingstone concluded that:

> *"Estimates for exposure to pornography online are lower than many anticipated – a quarter saw sexual images in the past year online or offline, and one in seven saw them online, rising to a quarter of older teens. Even assuming some under-reporting, it seems that media hype over pornography is based on unrepresentative samples or just supposition."*[13]

[11] http://www.talktalkgroup.com/press/press-releases/2012/07-02-2012a.aspx

[12] Livingstone, S., Haddon, L., Görzig, A., and Ólafsson, K. Risks and safety on the internet: the UK report. LSE, London: EU Kids Online. p. 8-9

[13] See http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-

We hope that the Government's child protection policy will be based on robust evidence, rather than the sort of 'unrepresentative samples or just supposition' that underpins much of the media's discussion of the issue. That should include an analysis of the scale of the problem, the context of those affected by it and the effectiveness and consequences of possible responses to it.

We do not mean to say that Internet access should be a 'free for all', or that children should face no restrictions on their Internet use, or that the state or businesses should play no role in keeping children safe online. We are instead suggesting that policy to tackle a problem should be based on a sound assessment of the scale and nature of this issue and the best responses to it, especially as these have consequences for other rights such as freedom of expression, for adults and young people.

> **Q10a: “A system in which some internet content (for example, pornography) is automatically blocked for you by your internet service provider or by the smartphone or other device you use to access the internet and you can later ask them to remove the filters if you want to access the blocked websites”**
>
> **Q10b: A system where you are automatically asked some questions about what you want your children to be able to access on the computer or other device (including pornography, but also including things like 15-rated films, information about drugs, and whether and when you'd like them to be able to access social networking sites). There would be no answers decided for you in advance (no defaults).**
>
> **Q10c: A system that combines (a) and (b), where you are asked all these wider questions in (b), but where for some obviously harmful content (like pornography), some of the answers are ‘ticked' for you in advance, so that if you don't change the setting as you are going through the questions, the content is blocked. You would still be able to change the answer if you wanted to.**

We support the model of active choice proposed in question 10b. We believe this approach will, if supported with good education and awareness measures, help parents best manage children's online access and the risks that come with it.

This is a position the Government has so far committed itself to. Picking up on Professor Byron’s concerns about parental responsibility, the 2011 Bailey Review recommended primarily an ‘active choice’ approach, and noted that:

> *“we would still want parents to be actively responsible for the safety of their children and take an ongoing interest in their use of the internet.”*

The Bailey Review recommended that the Government analyse the effectiveness of active choice ahead of proposing any further measures.[14]

Looking at the suggestion in question 10c, we question whether it will be possible to specify appropriate defaults that reflect some 'average' or basic set of options that will make sense for all families. How will this account for the differences between ages and parenting approaches across different families? Who will choose the defaults, and on what basis?

We certainly see no case for default 'on' filtering. In adopting any form of default blocking, whether a modified active choice or the option in 10a, the Government is making an assumption about what

11)/EUKidsOnlineIIReports/Final%20report.pdf page 42

[14] See page 14 https://www.education.gov.uk/publications/eOrderingDownload/Bailey%20Review.pdf

is 'blockable' and what categories of content are appropriate for households of all varieties. This is simply not possible.

An ‘on or off’ model cannot reflect the needs of such a broad age range. They are unlikely to match the needs of young people themselves, the wishes of their parents, or the compromises and decisions that children and parents should make together about Internet use.

Parents should be provided with the tools and resources to be able to manage this in the home. These are questions that parents themselves must answer.

It is also useful to consider the number of households this will effect. The ONS show there were around 7.5m families with dependent children in the UK in 2011, and around 10m without[15]. When considering costs and other consequences, it is important to consider that filtering aimed at protecting children is unlikely to be relevant for most households. We suggest this puts into question how appropriate default 'on' filtering will be.

From early this year there has been a sustained campaign for default-on blocking that has been most visible in the Daily Mail. This newspaper in particular has also suggested there is a groundswell of public opinion behind the idea of default filtering.

However, we have noted the survey conducted by YouGov which asked whether responders agreed with proposals to filter the Internet by default. The majority (57%) said they thought someones internet services should only be filtered if they ask for it. 36% said they thought that people's internet service should be filtered unless they ask for it not to be.[16]

This poll was inaccurately reported in the Daily Mail itself as establishing that the majority of responders *agreed* with plans for default 'on' filtering (claiming that 'two thirds of the public agreed with the Daily Mail campaign' that pornography should be blocked by default). The article has since been removed from the Daily Mail website[17]. We have seen no other polling or similar work to identify and analyse public opinion on default filtering that would suggest it is something the public is demanding.

DVD and TV regulation

We also note references to the TV watershed and classification system as examples of effective regulation of adult content. However, we would point to the evidence given by Professor Livingston to the Premier Christian Media sponsored inquiry, during which she argued that:

> *“24% had said that they had seen pornography, and in fact 16% said they had seen it on television, DVDs, and other sources, and 11 % said they had seen it on the internet.*
>
> *And we defined it for them as material that was obviously sexual, naked people and people having sex, those were the exact words, we didn’t give the children the word “pornography””*[18]

She continues later in the session:

> *“I would remind you that more children in Britain see pornography through television and*

[15] http://www.ons.gov.uk/ons/dcp171778_251357.pdf p. 4

[16] See http://d25d2506sfb94s.cloudfront.net/cumulus_uploads/document/bkmm9p70rl/YG-Archives-Pol-SundayTimes-results-27-290412.pdf

[17] See http://www.computeractive.co.uk/ca/computeractive-blog/2172485/thirds-public-common-sense-campaign-don-t-isps-block-websites

[18] http://www.claireperry.org.uk/downloads/independent-parliamentary-inquiry-into-online-child-protection.pdf p 43

> *DVDs than they said they had over the internet, I'm sure this is going to change but nonetheless I think people are more happy because they understand the system."*[19]

It should not be assumed that the existence of a watershed and ratings on physical media is an effective model to emulate, or that it is applicable to the Internet.

Disrupting the market for filtering services

Furthermore, where parents do want to install filters, there are a range of options available in a developing market for such services. Mandating network level blocking would add up to a very serious market intervention from the Government. This should be about making sure choices are available, and supporting parents to make their own.

There is a diverse and emerging market for tools – for example, we note the study by Dominique Lazanski that offers a non-exhaustive list of available filtering and monitoring tools[20]. Mandating network level blocks would be a serious intervention that will likely distort and undermine this.

Parents should be supported and educated to help them make the best decisions about what is appropriate for their own family. A market is developing to offer tools to help them do this. The Government's role should be to work with industry and parents to ensure there is clear information, guidance and advice about what is available so that those that want filters face few obstacles to setting them up.

Filtering as a means of protecting children and young people

Default filtering also makes assumptions about the *effectiveness* of filtering as a means of protecting children online. The EU Kids Online study noted above helps shed some light on the effectiveness of various forms of parental intervention in managing a child's use of the Internet and their exposure to risk online. This demonstrates the limitations of network-level filtering services on its own terms – of protecting young people from risks online.

In the EU Kids Online study noted above, the authors write that "we cannot investigate cause and effect but we can examine the associations among what parents do and what children say about online risk and harm." And on that basis they state that "technical mediation such as using a filter is not shown to reduce online risk encounters among children." They go on to conclude that "technical mediation has no significant impact between 9 and 14, and is associated with more harm for 15-16 year olds."[21]

The technical issues

There is no attention afforded in this consultation, as far as we can see, to the relative merits of different types of Internet filtering such as device, router and network level filtering.

Mandating network level filtering effectively encourages the further development of an infrastructure of censorship that could be prone to error, overreach or abuse. We note some of the issues to consider here, whilst also recommending the department conduct a full technical analysis comparing filtering options. Open Rights Group have prepared a short briefing which introduces the issues, available to download from our website[22].

[19] http://www.claireperry.org.uk/downloads/independent-parliamentary-inquiry-into-online-child-protection.pdf p. 55
[20] http://www.adamsmith.org/sites/default/files/research/files/parentledprotection.pdf
[21] http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20III/Reports/ParentalMediation.pdf
[22] http://www.openrightsgroup.org/assets/files/files/pdfs/Net%20Filtering%20Brief.pdf

First, ISP-filters can be subject to abuse or exploitation for reasons other than child protection, for commercial or political reasons. And it can be harder to manage problems such as mistaken blocking because the ISP acts as a further intermediary between the user and the filtering – an intermediary whose core commercial interest is not accurate filtering.

Second, there is a privacy risk**.** ISP filtering requires the ISP to monitor user traffic in some way. Often filtering tools are supplied to ISPs by third party companies, which means that details of Internet use are potentially gathered by those companies as well.

Third, ISP-level level filtering is unable to deal with user-specific filtering settings. It is not possible to account for different users on different devices in a single household (for example, children of different ages).

Fourth, it cannot filter TLS encrypted traffic. This means a filtering system risks becoming obsolete as a mechanism of controlling traffic as 'encryption' is more widely adopted.

TLS (SSL, or 'https') encryption is a way that traffic is made unreadable to intermediaries such as ISPs. It is widely used in online financial transactions, for example. But it is increasingly common in routine everyday Internet use. New browsers are built to check if encryption is available, and if so, to use it. As the cost of deployment for TLS falls it is expected to be used on an increasing percentage of websites. One might expect providers of adult content, for example, to be among those most motivated to implement TLS.

TLS makes it technically difficult for an ISP to filter traffic to a specific web address the user is visiting. That would make conventional ISP filtering obsolete. For example, BT's block of 'Newzbin2' does not stop people visiting 'https://www.newzbin.com' for this reason.

There are many other ways that users can 'get around' blocking using other forms of encryption or traffic 'tunnelling'. And it is important to recognise filtering is fallible in this sense. It will be pretty trivial to get around. For example, Ofcom also noted that:

> *“Circumvention of a block is technically a relatively trivial matter irrespective of which of the techniques used. Knowledge of how site operators and end users can work around blocks is widely distributed and easily accessible on the internet. It is not technically challenging and does not require a particularly high level of skill or expertise.”*[23]

Network level filtering does not fulfil its promise of reassurance that harmful content is blocked. Children may find routes around the filtering or the systems may simply fail to stop access to sites that parents may prefer their children not to access.

The managing director of filtering company Smoothwall also commented that:

> *“Blocking at the network level is a very blunt instrument. It may help to prevent young people coming across pornography unintentionally, but probably won’t stop those actively seeking it. Many other totally legitimate sites may be caught by the block as well.*
>
> *It’s unreasonable to expect ISPs to provide a solution to this problem working alone. All the stakeholders in industry and society need to be involved – especially parents who should be encouraged to have an active role in controlling what their children see.”*[24]

He touches on another crucial issue – as well as being trivial to get around, filtering systems tend

[23] http://stakeholders.ofcom.org.uk/binaries/internet/site-blocking.pdf

[24] http://www.ispreview.co.uk/index.php/2012/05/web-filtering-firm-smoothwall-warns-uk-not-to-force-net-censorship-on-isps.html

to block far too much content. That can be through errors, misclassifications or abuse. For example, in our study of mobile Internet filtering, we found all sorts of websites blocked that should not be. In our report we noted ten of those reported in the first few months of our monitoring:

> 1. ‘Tor’ (www.torproject.org). We established that the primary website of this privacy tool (meaning the HTTP version of the Tor Project website, rather than connections to the Tor network) was blocked on at least Vodafone, O2 and Three in January.
>
> 2. La Quadrature du Net (www.laquadrature.net/en). The website of this French ‘digital rights’ advocacy group was reported blocked on Orange’s ‘Safeguard’ system on 2nd February. La Quadrature du Net has become one of the focal points for European civil society’s political engagement with an important international treaty called the Anti-Counterfeiting Trade Agreement. The block was removed shortly after we publicised the blocking.
>
> 3. Shelfappeal.com was reported blocked on 15th February 2012 on Orange. This is a blog that features items that can be placed on a shelf.
>
> 4. Septicisle.info was reported on 7th February, and was blocked on Vodafone, Orange, and T-Mobile. This is a personal blog featuring political opinion pieces. It does not contain any adult content.
>
> 5. The Vault Bar (www.thevaultbar.co.uk) in London. We established that the home page of this bar was blocked on Vodafone, Orange, and T-Mobile on 6th February.
>
> 6. St Margarets Community Website (www.stmgrts.org. uk), is a community information site ‘created by a group of local residents of St Margarets, Middlesex.’ Their ‘mission is simple - help foster a stronger community identity.’ We established it was blocked on Orange and T-Mobile on 8th March.
>
> 7. eHow.com is an advice and educational site. It provides tutorials on a wide range of everyday issues, from ‘navigating after- school care’ to ‘small space garden tips’. We established it was blocked on Orange on 9th March.
>
> 8. Biased-BBC (www.biased-bbc.blogspot.co.uk) is a site that challenges the BBC’s impartiality. We established it was blocked on O2 and T-Mobile on 5th March. It is classified as a ‘hate site’ by O2’s URL checker
>
> 9. Yomaraugusto.com is the home page of a graphic designer, offering a portfolio of his art and design work. This was found to be blocked on Three and Orange on 6th February.
>
> 10. Exquisitetweets.com allows users to create one-page threads to save or share from conversations on Twitter. This site was blocked on Vodafone, Orange, and T-Mobile on 15th February.[25]

Since then we discovered the technology site GigaOM was blocked[26], as was the technology business advocacy group Coadec[27]. We continually receive reports of inappropriately blocked sites through our website, most recently about a range of sites associated with various sorts of birthing health and wellbeing advice.

[25] See our report on mobile Internet filtering, submitted alongside this response. Also available at http://www.openrightsgroup.org/ourwork/reports/mobile-internet-censorship:-whats-happening-and-what-we-can-do-about-it

[26] http://gigaom.com/europe/orange-overblocking-gigaom/

[27] http://www.newstatesman.com/blogs/voices/2012/08/problem-porn-filters

Some of these sites may include content that some parents would not want their children to see. Some of it should clearly not be blocked at all. The point is that parents are those best placed to make these decisions. Any form of default network level blocking involves assumptions that exacerbate the effects of filtering systems' tendency to over-block.

Our research also found that it can be difficult to opt-out of filtering systems, that it is too difficult to report mistakes and get them rectified, and that filtering systems lack transparency. The problems of over-blocking are compounded when it is not clear to consumers when filters are turned on, when it is difficult to report mistakes, and when it is difficult to opt out. That makes it harder to make sure that the filtering applies as far as possible to the right people at the right time.

As well as denying users affected by blocking access to perfectly legitimate sites, overblocking can disrupt legitimate businesses and organisations. The Internet is a potential platform for great social and economic innovation. One reason for this is that it lowers barriers to entry and makes it easier to bring a product or service to market. Over-blocking without easy forms of reporting or redress will see businesses being cut off from their market. It is likely that smaller, newer companies will be more likely to suffer, where they don't have the weight or popularity to demand reclassification.

This is especially problematic where classification, and therefore exactly what is blocked and why, is opaque. There are significant risks of deliberate market abuse, or for accidental harms to businesses that are cut off from segments of their market through misclassification.

Freedom of expression and why it matters

The UN Special Rapporteur for Freedom of Expression, Frank La Rue, is an expert appointed by the Human Rights Council to monitor the right to freedom of expression and opinion around the world. He noted last year that restrictions on access to information can have a '"chilling effect" on this right,' concluding that restrictions on access to information online must be:

- limited to exceptional circumstances;
- governed by law and a clear legal process;
- necessary and the least restrictive means required to achieve the aim.[28]

These principles are important because they limit the extent to which governments or businesses or others can limit the free access to information through overzealous efforts to protect citizens or more abusive attempts at limiting free access to information. In the context of child protection online, the Special Rapporteur finds that:

> *"Similarly, while the protection of children from inappropriate content may constitute a legitimate aim, the availability of software filters that parents and school authorities can use to control access to certain content renders action by the Government such as blocking less necessary, and difficult to justify.*
>
> *Furthermore, unlike the broadcasting sector, for which registration or licensing has been necessary to allow States to distribute limited frequencies, such requirements cannot be justified in the case of the Internet, as it can accommodate an unlimited number of points of entry and an essentially unlimited number of users."*[29]

[28] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, May 2011 p. 8

[29] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, May 2011 p. 9

Unintended consequences for children and young people

As noted above, filtering cannot replace involved and engaged parenting – and as noted already may induce a false sense of security on the part of parents and policy makers. This issue was highlighted by Professor Tanya Byron in her reports for the UK Government:

> *"...policies that claim to make the internet completely safe are undesirable because they discourage children and parents from taking an informed approach to managing the risks. At worst they can be dangerous – lulling parents into a false sense of security and leaving children exposed to a greater level of risk than they would otherwise be"*[30]

The age range covered by filtering encompasses a significant period of young people's development. Filtering could lead to children, young people, and adults being denied access to legitimate and age-appropriate information and resources such as sexual health information and advice.

The result is that filtering that covers such a range of young people and such a broadly defined set of 'adult' content can deny young people access to material appropriate to their development and needs. In a paper to the EU Kids Online conference last year, Tim Davies, Sangeet Bhullar and Terri Dowty argue that filtering can restrict young people's rights in the name of protecting them from risk – specifically "rights to freedom of expression and access to information across frontiers (Article 13, 17), rights to freedom of association (Article 14), rights to preparation for responsible life in a free society (Article 29) and rights to protection of privacy (Article 16)". They argue that:

> *"...these broader rights are frequently neglected - with young people's access to information on key topics of health, politics and sexuality limited by Internet filtering - and with a lack of critical formal and informal education supporting young people to gain the skills to live creative and responsible lives in increasingly digitally mediated societies."*[31]

This was echoed by Children's Rights International Network. Jenny Thomas, Senior Child Rights Officer at CRIN, wrote that:

> *"Children's rights advocates quite rightly fear that imposing broad restrictions on children's access to information couched in arguments about child protection not only contributes to discrimination against certain groups - most often sexual minorities - but that such blocks also serve to deny children age-appropriate information about issues such as sex education, sexuality and drug use.*
>
> *This is information to which children have a right, and which can support them to make informed choices. In this way, providing children with information clearly contributes to, rather than detracts from their right to protection."*[32]

Q16a: "What is your business / trade assoc doing to ensure parents have access to a range of simple tools and information"

We would note here our research into mobile Internet filtering that is referenced above. We have submitted the report alongside this response. The Government should look at the broad effects of

[30] See Professor Tanya Byron, 2008, Safer Children in a Digital World: The Report of the Byron Review, http://media.education.gov.uk/assets/files/pdf/s/saferchildreninadigitaworldthe2008byronreview.pdf page 81

[31] See Tim Davies, Sangeet Bhullar, and Terri Dowty, "Rethinking responses to children and young people's online lives", September 2011

[32] http://zine.openrightsgroup.org/features/2012/firewalling-child-rights-in-the-name-of-protection

existing systems and the benefits and problems associated with them.