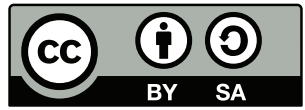
Mobile Internet censorship:

What's happening
and what we can do about it.

This is a joint publication from Open Rights Group and the LSE Media Policy Project. Published under Creative Commons license Attribution Share-Alike.



May 2012.

LSE Media Policy Project: *http://blogs.lse.ac.uk/mediapolicyproject*
Open Rights Group: *http://www.openrightsgroup.org*

by Peter Bradwell, Gemma Craggs, Alessandra Cappuccini and Joana Kamenova.

Contents

Introduction

In late December 2011 Open Rights Group launched the website Blocked.org.uk. It gives people an easy way to report when sites and services are 'blocked' on their mobile network.

A 'block' means that the mobile company prevents a user from connecting to a given site. By default, mobile phone companies currently filter Internet access on their pre-pay accounts in this way. Essentially, anybody with a mobile phone account with these filtering systems in place will not be able to access websites that the mobile operators consider unsuitable for under 18s. The material that is blocked is far broader than just adult sexual content.

We think there are a number of serious problems with how these systems work. These include a lack of transparency, mistakes in classifying sites and the difficulty of opting out of the filtering. Together, these problems mean that people often find content is blocked when it shouldn't be.

The result is that filtering systems designed to give parents a way to manage their children's access to the mobile Internet actually affect many more users than intended and block more sites than they should.

This is the nature of our concern. Mobile operators are dealing with

difficult questions and by no means get everything wrong. However, at present the filtering systems are too blunt an instrument and too poorly implemented. Mobile Internet filtering blocks too much content, and applies to too many people, meaning it effectively adds up to a system of censorship across UK networks.

As more people use mobile devices to access the Internet, and as the Internet continues to provide a potential platform for promoting both freedom of expression and economic innovation, it is critical that such problems are addressed. If they are not, then this form of censorship will continue to create unwanted restrictions on access to information for adults and young people, which will damage markets, undermine the free flow of ideas and open communication, and make it harder to promote responsible Internet governance internationally.

Mobile companies should be aiming to reduce to zero the number of adults who have either unintentional or unwanted parental control filters on their accounts. They should be able to achieve that while still helping parents manage their children's access to the mobile Internet.

In this short briefing we set out our perspective on the problems. We explain how mobile Internet filtering currently works, point out some of the consequences, and suggest ways that these problems might be addressed. We believe that taking decisions about what people can access online out of their own hands requires following some simple principles. Filtering controls must be clearly and transparently implemented. They should be responsive to mistakes, be easy to opt out of and involve an active choice to opt in.

Our conclusions are based on the reports we have received through Blocked.org.uk and from 'mystery shopper' calls we have made to mobile networks. In these we complained about incorrectly blocked sites to the mobile operators and assessed the response (see appendix 1).

1. What's happening

Mobile data access has become an integral part of our connected lives. According to Ofcom, 28% of UK adults said they accessed the Internet on their mobile in the first three months of 2011, and mobile data use increased forty-fold between 2007 and 2010.[1]

A survey by Childwise, of almost 2,500 children and young people aged 5 – 16 in over 100 schools across the UK, found that 44% of children aged 5 – 10 and 95% of children aged 11 – 16 owned a mobile phone. 25% of all children with a mobile phone access the Internet through this device.[2] Another survey, funded by the EC Safer Internet Programme and led by Professor Sonia Livingstone from LSE, of over 1000 UK children and their parents or guardians found that half of those children aged between 9 and 16 reported going online via a mobile device.[3]

Concerns about the content that young people are able to access have increased as swiftly as access to the Internet and new technology

When looking at young people's experiences of risk online, the same researchers 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.[4]

When considering the best way for young people and their parents to deal with online risks, including exposure to undesirable content, the same Europe-wide study 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,'*[5]

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.[6]

Parents' perceptions and the mobile operators' response

Parents do share real anxiety about young people's access to the Internet. According to the Bailey Review, which looked at the commercialisation and sexualisation of children in 2011, 23% of parents think it likely that their child will experience something that bothers them online in the next six months.[7] Similarly, Ofcom found that in 2010 26% of parents were very or fairly concerned about the content of websites their children were visiting.[8]
Phone companies 'censor' the mobile Internet by default because

they don't know whether their phones are being given to or used by children and young adults. The concern is that unfettered access to the Internet might mean they stumble upon undesirable material. Adults must prove their age in order to access 18-rated content.

2. What is the problem?

Making sure parents have the tools to give their children safer access to the mobile Internet is a worthwhile goal. Service providers should help them when they seek ways to manage their children's use of technology. However, the tools to manage access to content are fallible. To understand why, it's necessary to explain how filtering works.

Filtering can be based on either a 'blacklist' or a 'whitelist' of websites. A whitelist is a list of sites that a filtering tool allows the user to see. Whitelists tend to be small and therefore well categorised. They are better suited to younger users, but do not scale well. A blacklist is a list of sites that a filtering tool should block. Given that there are millions of websites, blacklists are typically created through some form of automated classification process, and are prone to errors.

There are four key problems with how mobile blocking currently works.

First, sites may be incorrectly classified. Over-blocking catches sites that should not be restricted as part of a parental control service. Second, mobile phone operators are not transparent enough about how their filtering systems work or the kind of content they block. Third, it is often not clear how to report mistakes and problems.

Finally, it is sometimes difficult even for adults to turn the filtering off. The result is that a system ostensibly designed to help parents manage their children's access to the Internet is effectively implementing much broader restrictions on access to information that affect a much wider group of people than intended.

1. Filters often catch the 'wrong' content

Mobile filtering is mainly implemented through blacklists. The filtering system itself is often a product developed by a specialist Internet filtering company.

Sometimes filtering systems can lead to the wrong people being denied access to the wrong content. That can happen through mistakes, if a site is incorrectly categorised, or through abuse, if a site is deliberately added to a blacklist for reasons other than the stated purpose of the blocking. Mobile networks in the UK are more likely to suffer from mistaken blocking than deliberate abuse.

When the wrong content or site is blocked by a filtering system, it is called 'over-blocking'. In Australia, for example, it was reported that "a Queensland dentist, a tuckshop convener and a kennel operator have been included on a secret "blacklist" of sites to be banned by Australia's communications watchdog."[9]

In the past few months we have been contacted by members of the public about sites they considered were blocked incorrectly by mobile Internet filtering in the UK. They also reported that they found the response from mobile networks was inadequate when they tried to report problems such as incorrectly applied blocks. Some did not want filters completely removed, but found some sites blocked that they felt should not be.

For example, O2 blocked the website of a Sheffield church throughout the second half of 2011, claiming it features adult content.[10] The

church member who noticed the blocks tried to report the error, and at first all he managed to achieve was getting the blocks on his own phone removed – with a text informing him he could 'now access 18-rated content'. He was told that the church website itself could not be removed from the filter.

The story illustrates a number of key issues. First, although the blocks tend to be described as being for adult content, implying adult sexual content, in fact they apply across a much broader spectrum of material. Second, often the customer services teams are not well briefed on the issues and as a result seem unhelpful. Third, it is difficult if not impossible for a site that considers itself to be blocked incorrectly to have itself removed from the filter.

Blocked.org.uk

Following these reports, we wanted to understand the scale of the over-blocking problem. To help do this, we created a reporting tool that allows people to submit reports of blocks they consider to be inappropriate.

Working with a small group of volunteers, we collected over 60 reports of incorrectly blocked sites between 1st January and 31st March 2012.[11] The reports included bars and personal and political blogs through to political advocacy sites. These are ten examples of reports of inappropriate blocks we received via Blocked.org.uk:

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.[12] 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.

What is clear is that the blocking extends well beyond adult sexual content. And it is important to recognise that what is 'appropriate' is not at all easily defined, leaving many of the reports in a grey area.

There are two separate types of over-blocking. First, there are clearly many misclassifications, where sites are mistakenly placed behind a filter. For example, we found that a site advertising holiday villas in Portugal (*'www.algarve-beach-life.com'*) was blocked on Vodafone. This is presumably an error. Likewise, we hope, the block on access to La Quadrature du Net was in error.

Second, there may be disputed classifications, where deciding what material should be considered 'blockable' requires a subjective judgement. For example, some networks consider that forums should always be blocked, because of concerns that young people will interact with people they don't know. However, such a policy could cut off informative education forums, or may restrict young people's access to sites where they find support from their peers. The subjectiveness of such a decision is especially problematic given that the needs of 16-year-olds are very different from those of 11-year-olds, and that different parents will have different ideas about what is or is not appropriate at different ages.

It is hard to understand exactly how content is classified

Mobile operators all say that they act according to a code of conduct set by the Mobile Broadband Group.[13] But this code does not itself provide any criteria for determining or defining 'blockable' content. It does point to a framework devised by the Independent Mobile Classification Body[14] (IMCB).

Furthermore, that framework is explicit that 'content accessed via the Internet' lies outside of its remit and that of the IMCB.[15] As a result, the Mobile Broadband Group code of conduct that mobile operators adhere to states that filters are 'set at a level that is intended to filter out content approximately equivalent to commercial content with a classification of 18.'[16]

There is therefore a process of interpretation, as mobile operators look to derive blocking lists from the framework specifications. There is an added layer of interpretation: these filtering lists are usually maintained by the external third-party providers of the filtering systems.

There is a further problem of how 'current' the frameworks are. The IMCB Framework to which mobile operators adhere in their filtering policies was written in 2005. The latest version of the code of practice on self-regulation was published in 2009, with the original published in 2004.

It is not clear how frequently the mobile operators, individually or collectively through the Mobile Broadband Group, review how appropriate the filtering classifications are, or more broadly the effectiveness of their filtering systems.

Why over-blocking is a problem

Over-blocking is a problem in itself. It can mean a business is cut off from a slice of its market. It can simply see people unable to get directions to a bar. It may stop a prominent political organisation from reaching concerned citizens. We discuss these consequences further below.

However, 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.

To help understand how mobile operators respond to problems with filtering systems, we conducted a 'mystery shopper' exercise, calling four of the major mobile operators and reporting incorrectly blocked sites (see appendix 1 for more details). This helped us to identify three further problems.

2. A lack of transparency

First of all, there is currently a transparency problem, meaning that it is not clear enough when and how mobile Internet filtering is happening.

Mobile operators do not make it clear enough that blocking is turned on by default. The first that many users know of blocking on their account is when they come across a blocked site. For those who run websites subject to filtering, it is not easy to establish whether and why their site is blocked.

It is also not clear who it is that runs the mobile operators' filtering systems, and how their systems work.

3. Reporting problems and addressing mistakes

Mobile operators' staff often seem uninformed about mobile Internet filtering, and thus poorly trained to help users making complaints - whether they are trying to report a mistaken block or have blocking removed.

Furthermore, a customer's request to have the filtering removed may be framed as a request to turn on 'adult content' – which suggests the primary interest is adult sexual material. That ignores the breadth of the content blocked under these filtering systems.

4. It can be difficult to opt-out

Getting mobile operators to turn off blocks often requires consumers to provide credit card details as a means of identification or to go to a store. For many this may not be too onerous or problematic, although some may not want to provide credit card details either over the phone or through the page returned to a user when a site is blocked.

A more significant concern may be finding a way for those who run website they believe have been incorrectly blocked to 'opt-out. It is not at all clear that it is possible for sites to have themselves removed from content filters.

O2 offers a URL checker that reveals how a given site is classified, and offers a reporting button to request reclassification.[17] However, it is not clear what happens when a site is reported as incorrectly classified, and there is no route to directly report a website operator's concern. The URL checker also does not seem to be referenced or advertised anywhere on the O2 site or elsewhere.[18] Other operators do not seem to offer any such mechanism.

It is important to note that the mobile operators' policies vary, and some provide more and clearer information than others.

For example, Orange provides a list of the categories blocked under their 'Safeguard' system and a reasonably clear and comprehensive explanation on their website of why the system is in place.[19]

O2's explanatory page on filtering says that content is automatically classified according to criteria aligned with the IMCB classification framework, and the company offers two ways to report mistakes: Twitter and their online forums.[20] They also note which company provides their age verification system (Bango). However, as noted above there is no mention of their 'URL checker'.

This adds up to a general failure to provide mechanisms to report in a

way that would lead to the issues being addressed.

This report does not provide a detailed analysis of each operator's practices with the aim of rating and comparing them. But it is clear that all the systems in use by the mobile operators suffer in some respects from these four issues.

3. The consequences

The UN Special Rapporteur for Freedom of Expression, Frank La Rue, is an independent expert appointed by the Human Rights Council to monitor the right to freedom of expression and opinion around the world.[21] He noted last year that restrictions on access to information can have a '"chilling effect" on this right,'[22] 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.[23]

The importance of making sure that any filtering or censorship is minimal and respects such principles has recently been acknowledged by the UK Government. In a response to freedom of expression advocates including Open Rights Group, the Foreign Secretary William Hague reaffirmed the Government's commitment to freedom of expression online. With regard to child protection online, he said:

> *"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."[24]

However, current mobile filtering in the UK fails against all three principles laid out by Frank La Rue. It is overly broad, and governed by informal industry frameworks and contractual relationships with filtering service providers.

Handing power over what information people can access, or over the visibility of certain kinds of information, without following these principles has a number of consequences.

Restricting fair markets

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.

Censorship

There are clear problems for free access to and sharing of information when decisions about access are taken out of people's hands, and

left to opaque and informal agreements or clumsy and unresponsive technical systems. This is especially problematic in a filtering system that is not 'granular' enough, leading to blanket filtering that covers far too much material, for example sites such as restaurant sites, blogs about shelves, or political discussion sites.

Furthermore, if online censorship is widespread and accepted with little opposition as a way to implement a broad range of public policy issues, it becomes far harder to argue for Internet freedom elsewhere. Other governments and companies around the world use the same technologies to restrict access to online material and offer the same arguments about taste, decency and citizens' safety. This makes it harder to live up to the standards set out by Foreign Secretary William Hague throughout the past 18 months, including the letter mentioned above and his statements at the London Conference on Cyberspace in November 2011.[25]

Unintended consequences for young people

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 definitioned 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 therefore restrict young people's rights in the name of protecting them from risk – specifically "rights to freedom of expression and access to information across frontiers (Article 13, 17), rights to freedom of association (Article 14), rights to preparation for responsible life in a free society (Article 29) and rights to protection of privacy (Article

16)". They argue that:

> *"…these broader rights are frequently neglected - with young people's access to information on key topics of health, politics and sexuality limited by Internet filtering - and with a lack of critical formal and informal education supporting young people to gain the skills to live creative and responsible lives in increasingly digitally mediated societies."*[26]

These comments help emphasise one of the key problems for mobile Internet filtering as it currently works: it is not 'granular' enough. An 'on or off' model cannot reflect the needs of such a broad age range. Decisions about what counts as '18 rated' material are taken by mobile operators interpreting a broad code of conduct, and implemented by the third parties who run the classification and filtering systems. So they are unlikely to really match the needs of young people themselves, the wishes of their parents, or the compromises and decisions that children and parents make together about Internet use.

A false sense of security

It is worth noting that as well as blocking too much content, for the wrong people, 'ISP-level' filtering can also fail to achieve its stated goal of helping protect children from risks online. 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. Furthermore, filtering cannot replace involved and engaged parenting – and 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"[27]

For example, parents may not be aware that network-level blocking systems are unable to selectively filter 'encrypted' traffic. 'Https' encryption is a way to make traffic unreadable by intermediaries such as ISPs. It is widely used in online financial transactions, for example. It is also increasingly common in routine, everyday Internet use. New browsers are built to check if encryption is available, and if so, to use it. Encryption makes it impossible for an ISP to 'check' the web address the user is visiting.

For example, recently BT was ordered by a court to block customers' access to 'Newzbin2'. But that does not prevent people from visiting 'https://www.newzbin.com'.[28] There are many other ways that users can get around blocking using other forms of encryption or traffic 'tunnelling'.

Encryption is a technical choice made by site operators, rather than something users can unilaterally choose to turn on. For example, it is a necessity for protecting financial and other transactions online involving information that needs to be kept confidential. Outside of those categories, it is possible that the sites most likely to deploy 'https' will be those that most legitimately fall within a 'blockable' category.

Many of the problems noted in this report are associated with filtering at the 'network level' – meaning filtering run by service providers, in this case mobile operators. Control over what is blocked and why rests ultimately with them. This means the onus is on the service provider to communicate to users what filtering is happening on their networks.

It is important to recognise the limitations of network-level filtering services on their own terms – of safeguarding young people from risks

online. The debate about filtering the Internet is not simply about whether any effort is being taken to protect children. The point is that these efforts need to reflect the evidence surrounding young people's experiences of risk, and the technical and other issues regarding the workings of the filtering systems. This is a position the government has so far reflected. Picking up on Professor Byron's concerns about parental responsibility, the 2011 Bailey Review recommended 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."* [29]

4. Our 'asks' of mobile operators

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'.

Parents trying to manage their children's use of mobile Internet need support. Some simple changes to how mobile operators run their filtering services would help address many of the problems with mobile filtering. It should be possible for adults to be able to make choices about whether to activate on their accounts without undermining parents' ability to manage their children's use of mobile phones.

In the longer term there should be an effort to move away from filtering at the 'ISP level' towards device-based filtering. As a general rule, the closer to a user the filtering happens, the more control the user has over it.[30]

In the shorter term, we have recommendations across three main themes – choice, transparency, and redress and review.

1. Choice

1.Every adult should be given a straightforward choice at sign-up whether they wish censorship or not. This is often called an **'active choice'**. People should be able to specify when signing up to a mobile phone contract whether the content filtering is on or off. Ideally there should be no 'default' option – customers should have to actively say yes or no to the filtering option. This was recommended in last year's 'Bailey Review' into the commercialisation and sexualisation of children:

> *"...when a new device or service is purchased or contract entered into, customers would be asked to make an active choice about whether filters should be switched off or on..."*[31]

2. The framing of the question is important. These tools should be called **'parental controls'**, and the term 'adult content' should be avoided. The range of material caught stretches far beyond sexual content and the terminology should reflect this.

2. Transparency

1. Every adult should be given **clear advice about the kind of content that may be blocked**, and be provided with clear information on how the blocking works.

2. This should include information about **who provides the filtering technology** if a third-party supplier is involved.

3. Every mobile operator should provide **clear and easy ways to check if a site is blocked**. Website operators need to be able to check whether their sites are blocked, how their sites are categorised, as well as the criteria for classification and who was responsible. Such information would ideally be provided through a tool that allows

checking across all the mobile networks.

4. Every mobile operator should provide **easy ways to complain about wrongful blocks, including at the time when an incorrectly blocked website is found**. Since many customers are locked into the substantial contract terms attached to many phones, there must be robust reporting mechanisms and swift remedies so that customers can fix problems when changing provider is not an option. The threat of the customer's eventual departure will act as an incentive. Efficient remedies and customer service should be the norm regardless.

3. Redress and review

Mobile operators should regularly **review the performance of filtering** and open up the process of deciding what is blocked and how. While operators should be applauded for making the effort to establish pragmatic solutions for parental control, updates and reviews of codes and practices should happen more than once every few years.

The review process should be **a more open conversation about how these tools should work**. As content delivery and means of access change rapidly, it is important that codes of conduct, frameworks, and oversight are as up-to-date as possible.

This open conversation should extend to considerations of what content these filtering systems should block.

There need to be **mechanisms that allow website owners to challenge a refusal to remove their site from a blocking system**.

The Mobile Broadband Group should **review policies on blocking against benchmarked levels of performance** regarding transparency, choice mechanisms, and complaints and customer service procedures. There should also be a review of customer

awareness of and interest in filtering, matched against the numbers of users who have actively opted out.

At the same time, there should be **transparent reporting mechanisms** for problems, mistakes and resolutions.

5. What's 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. Badly implemented and over-broad filtering systems take back that power from people and place decisions about access to information under the control of informal industry agreements or over-broad and unresponsive filtering systems.

This is an issue that currently affects mobile broadband and needs to be addressed as soon as possible. However, the problems identified read across to Internet access in general. A number of proposals are developing to implement wider filtering systems for fixed-line broadband Internet access in the UK, including not only proposals for similar forms of child protection filtering, but also for filtering content related to terrorism and extremism and for copyright enforcement.

For example, in a speech to the Royal Television Society in September 2011, Jeremy Hunt set out plans to 'protect consumers from offensive and unlawful content'.[32] The Communications Bill, due to be announced in the Queen's Speech in 2012, will include new proposals for Internet filtering to protect children.

If they follow a similar blueprint of ISP level filtering as mobile operators, all the problems we have highlighted would be reproduced at a larger scale. For example, most fixed-line connections are shared by a number of people using a variety of devices. Implementing filtering in that situation would require a range of approaches from whitelisting for young children to censorship-free connections for adults.

Therefore, we hope that if the government does pursue such a policy it will be flexible, concentrate on users and devices rather than networks, allow the tools to be properly described as "parental controls" and above all avoid turning on blocking by default.

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.

What mobile filtering already helps to demonstrate is 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.

Notes

1 http://consumers.ofcom.org.uk/2011/08/a-nation-addicted-to-smartphones/

2 Research Highlights for Children's Online Safety #16, http://media.education.gov.uk/assets/files/pdf/1/16%20%20%20trends%20in%20media%20use.pdf

3 Livingstone, S., Haddon, L., Görzig, A., and Ólafsson, K. (2010). Risks and safety on the internet: the UK report. LSE, London: EU Kids Online. *p. 7* http://eprints.lse.ac.uk/33730/1/Risks_and_safety_for_children_on_the_internet_the_UK_report.pdf

4 Livingstone, S., Haddon, L., Görzig, A., and Ólafsson, K. (2011). Risks and safety on the internet: the UK report. LSE, London: EU Kids Online. *p. 8-9* http://eprints.lse.ac.uk/33730/1/Risks_and_safety_for_children_on_the_internet_the_UK_report.pdf

5 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, http://www2.cnrs.fr/sites/en/fichier/rapport_english.pdf

6 See "Safer Children in a Digital World: The Report of the Byron Review", 2008 http://media.education.gov.uk/assets/files/pdf/s/safer%20children%20in%20a%20digital%20world%20the%202008%20byron%20review.pdf and "Do we have safer children in a digital world? A review of progress since the 2008 Byron Review", 2010 http://media.education.gov.uk/assets/files/pdf/d/do%20we%20have%20safer%20children%20in%20a%20digital%20world%202010%20byron%20review.pdf

7 The Bailey Review, 2011, http://www.education.gov.uk/publications/standard/publicationDetail/Page1/CM%208078 *p. 36*

8 UK Children's Media Literacy, Ofcom, 2011, *p. 66*, http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/media-lit11/childrens.pdf

9 http://www.couriermail.com.au/news/web-blacklists-innocent-victims/story-e6freon6-1225698047112

10 http://www.openrightsgroup.org/blog/2011/o2-bans-church-this-christmas

11 A full list of the reports submitted to Blocked.org.uk between January 1st and March 31st can be found at www.openrightsgroup.org/assets/files/files/BlockedReports.xls

12 http://www.openrightsgroup.org/blog/2012/orange-uk-blocking-la-quadrature-du-net

13 http://www.mobilebroadbandgroup.com/documents/mbg_content_code_v2_100609.pdf

14 http://www.imcb.org.uk/

15 http://www.imcb.org.uk/~/media/Files/IMCB/ClassificationFramework.pdf, *p. 4*

16 http://www.mobilebroadbandgroup.com/documents/mbg_content_code_v2_100609.pdf

17 http://urlchecker.o2.co.uk/urlcheck.aspx

18 The only mention we could find of the URL checker was on a GiffGaff forum: http://community.giffgaff.com/t5/Submit-Great-giffgaff-Ideas/Have-a-data-bar-that-doesn-t-include-the-giffgaff-site/idi-p/328329/page/3

19 http://help.orange.co.uk/orangeuk/support/personal/480083

20 http://blog.o2.co.uk/home/2011/03/mobile-phones-and-age-verification-your-questions-answered.html

21 http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/OpinionIndex.aspx

22 See Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf, May 2011 *p. 8*

23 See Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf, May 2011 *p. 6-16*

24 The Foreign Secretary's reply on UK Internet freedom, Open Rights Group blog, January 05, 2012 http://www.openrightsgroup.org/blog/2012/the-foreign-secretarys-reply-on-uk-internet-freedom

25 See the Foreign Secretary's closing remarks, http://www.fco.gov.uk/en/news/latest-news/?view=Speech&id=685672482

26 See Tim Davies, Sangeet Bhullar, and Terri Dowty, "Rethinking responses to children and young people's online lives", September 2011, http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/Conference%202011/Davies.pdf

27 Professor Tanya Byron, 2008, Safer Children in a Digital World: The Report of the Byron Review page 81, http://media.education.gov.uk/assets/files/pdf/s/safer%20children%20in%20a%20digital%20world%20the%202008%20byron%20review.pdf

28 Newzbin recently moved to newzbin2.es

29 The Bailey Review, 2011, http://www.education.gov.uk/publications/standard/publicationDetail/Page1/CM%208078 *p. 38*

30 For more information, see our briefing on types of filtering: http://www.openrightsgroup.org/assets/files/files/pdfs/Net%20Filtering%20Brief.pdf

31 http://www.education.gov.uk/childrenandyoungpeople/healthandwellbeing/b00743115/bailey-review, *p. 38*

32 See http://www.culture.gov.uk/news/news_stories/8431.aspx

Appendix 1: 'Mystery Shopper' results

We contacted the customer services numbers for four major mobile phone networks, Orange, T-mobile, Vodafone and 3, to look at how they deal with complaints about their Internet filtering systems. Using a set script (see below), two volunteers posed as a genuine customers and contacted each mobile network to report a block they wanted removed from their pay-as-you-go phones. They asked for the site to be removed from the filtering system.

As noted above, defining 'incorrectly' blocked sites is difficult considering the variety of ages filters are designed to cover and the judgement involved in deciding what content is 'appropriate'. So it is not possible to say we were reporting sites that were unquestionably inappropriate. Rather, these were edge cases

Our volunteers recorded how the mobile operators handled the complaint. Each operator was called once – meaning these results are indicative, and not repeat-tested. They suggest a lack of knowledge and a lack of consistency on the part of the mobile operators' representatives, resulting in a lack of transparency and responsiveness to consumer requests.

Orange

We contacted Orange to report the blocking of *'www.thevaultbar.co.uk'* – the website of a bar in Woodford Green.

The Orange representative made no effort to ascertain what site we were trying to access. We informed Orange that the website contained no adult material and questioned why it had been blocked.

We were told that sometimes sites are 'just blocked' by the Orange Safeguard settings and that there was nothing that could be done about it. We were told we could have access to the site if we unblocked the phone entirely, and that unblocking one site alone was not an option. There was no mention of a reporting mechanism for incorrect blocks.

T-Mobile

We reported the blocking of *'www.thetruthseeker.co.uk'* to the T-mobile representative.

T-Mobile also did not ask which website we were trying to view. We explained that the site was a blog, contained no adult material and therefore should not be blocked. T-Mobile told us that the content block is on by default. The explanation went no further.

We were then asked if we could access other Internet sites, which we could. The representative then concluded that the content block was working correctly, despite our insistence that we were not trying to view adult material. There was no option to unblock the site; we would have had to remove the content filter entirely if we wanted access to restricted sites, once we had satisfied the age verification procedure.

Nevertheless, even though we did not provide age verification in any form, after the phone call our pay-as-you-go phone had the content filter removed.

Vodafone

We contacted Vodafone to report the blocking of *www.torproject.org*. This is the home of the anonymiser Tor, and provides information about the service.

Vodafone, again, did not ask what website we were attempting to unblock. We told them that in fact it contained no adult material. They checked to see if our phone had age restriction in place and asked if we could access other websites. We stated that we could but repeated that the blocked site contained no adult material.

Vodafone explained that website blocking is done by default and that many websites are blocked. The representative described it as 'random' and the 'luck of the draw'.

When pushed as to why sites with no adult material on were being blocked, the representative stated that it was to protect children. Again, we were advised that the content filter could be removed from our phone once we had provided age verification. However, midway through the conversation the customer service representative did state that I 'sounded' over 18 and was initially willing to remove the age restriction filter immediately.

3

We reported to 3 that the site *melonfarmers.wordpress.com* - a conspiracy theory discussion site - was blocked.

The customer services representative asked what message we received when trying to access the site. We told them we were shown a blocking screen telling us over-18 blocking was enabled. We were advised that 'adult sites' were automatically blocked on all pay-as-you-go 3 mobile phones.

However, we were not asked what site we were attempting to access, despite our insistence that it contained no adult material. We were then asked if we were having issues accessing other sites like Google or the BBC, and replied no. Again, the representative concluded that the content filter was working correctly and that the site we were trying to access must have some sort of adult material on it, hence its blocking.

When we asked 3 how the company classifies blocked websites, the representative told us that 3 does not make the rules, and that 'the government' does. We were also informed that no record is made of sites which are reported as incorrectly blocked and our phone would be unblocked once we provided age verification.

O2

We reported to O2 that the site w*ww.normanfinkelstein.com* – the personal homepage of a political writer and lecturer – was blocked on 18th February 2012. The representative said they were not sure why this particular site was blocked. They also did not know why it would be blocked despite not containing any adult content.

They told us that if it was blocked on one account then it is blocked on everybody's phone, and did not suggest a way for us to access that site without turning the filtering off completely.

To opt out, we were asked to call 61018 with credit card details or go to an O2 shop. They were unaware of any other ways to opt out.

They apologised for not being able to help, but did not forward us to anyone that could.

Implications

Lack of transparency regarding how mobile filtering systems work

All the networks have a default filtering system in place on their pay-as-you-go phones. But none of them offered satisfactory reasons why inaccurate blocks happen.

The mobile operators generally assumed that because we had access to other 'friendly' sites (BBC / Google) that their filtering systems were working correctly. This is despite the fact that we deliberately used examples of a non-adult material related website as our test site.

Perhaps the most unusual of all the explanations came from 3, whose representative seemed to be under the impression that 'the government' set the standard for adult content filtering. This is incorrect; each mobile network uses a third party to classify and filter websites against a framework set by an industry body.

Is there a system to record and amend incorrectly blocked websites?

None of the mobile phone operators asked what websites we wanted to unblock, suggesting that they are not offering to record sites that are being incorrectly blocked.

As a results, sites are only 'unblocked' because a user's phone has filtering removed, instead of removing erroneous blocks from the whole network. This calls into question whether mobile phone networks actually consider inaccurate site blocking an issue. Incorrect blocking negatively affects the end user and the website in question, as both are having their access limited by inaccurate website filtering systems.

Is there a consistent age verification process that respects privacy?

Networks asked for either a driver's licence or a credit card number. Failing that, customers are required to go to mobile operators' high street stores.

During our conversation with Vodafone we were told that we 'sounded' over 18 and that the representative could remove the block on that basis. T-Mobile removed the website filtering system from our phone completely, opening access to any website.

Do mobile operators provide a way of unblocking an incorrectly blocked website?

They only solution we were offered was the complete unblocking of our phone. This is not an option for adults who share their phones with their children or occasionally let them use it, or for website managers responsible for incorrectly blocked site.

Mobile networks seemed to offer complete removal of the adult filter, even though in our tests we were not asking to have access to sites that warrant age verification.

Script used in calls to mobile operators

1. Do you know why this particular website has been blocked, as it does not contain any adult related content?

2. How do I get this block removed?

- I do not want to provide credit card/address or driving license details. How do I go about this?
- Going into a phone shop is pretty time consuming / great inconvenience.

3. If this blocking filtering system is automatic, then why has this website, with no adult-related material, fallen within the parameter of being blocked?

4. How long will it take for this block to be removed?

5. Is the site just going to be unblocked on my phone, or will everyone now be able to now access it due to my complaint?

6. Does this website get reported/how do you manage these incorrectly applied blocks/complaints?

7. I share my phone with a child/minor so I CANNOT have the content filtered completely removed. But I do need access to the site I am requesting.


OPEN
RIGHTS
GROUP


LSE MEDIA
POLICY
PROJECT
Promoting media policy communication
between academics, civil society
& policymakers