Parental Internet Controls

Response to Consultation

Geoff Richards

6 September 2012

1 Introduction

I am submitting this consultation response as a PDF document with my own choice of section structure. This is for two reasons:

- I was unable to fill in the form provided as a Word format document, since I don't have a copy of Microsoft Word. I was able to use LibreOffice to view the document, but it doesn't seem to support filling in the form parts.
- The form provided has questions relevant only to parents and businesses such as ISPs—of which I am neither—and it doesn't touch on the areas which I think are problematic with the proposals.

I am an adult who uses the internet for many things, and feel no need to have parts of the internet blocked to protect me personally from harm. No children have access to my broadband connection. I also run a small (non-pornographic) personal website, and have helped create websites for other individuals and small to medium sized businesses.

The fact that the consultation doesn't address the issues I have with a default-on network-level filtering regime is all the more reason to make the UKCCIS aware of them. The technical issues, and the consequences of this kind of filtering, should be considered carefully before proceeding. I fear that a desire for a simple solution to address the concerns of their members has led them to fail to appreciate the actual complexity of the proposals.

My main concerns derive from the intention that network-level filtering by ISPs will be used. If computers were sold with web filtering software pre-installed, and set to offer the user different filtering options when

they first booted up, then most of the potential problems discussed below would be mitigated or avoided.

2 Defining Objectionable Content

The consultation offers no definition of what is meant by 'pornography', which leads me to wonder who will decide what will be included in the content restricted from people with filtering enabled. The answer would seem to be 'the people who make the software that the ISPs decide to buy'. That hardly seems sufficient when dealing with such a divisive subject. Some people would expect anything remotely titillating to be blocked—such as YouTube videos of scantily clad pop-stars—while other parents might consider artistic nude photographs to be acceptable for viewing even by their children. Unless specific definitions can be given we are likely to see a lot of disagreements, legal action, and angry campaigns for ever more content to be filtered out by ISPs.

The same ambiguity may arise with other kinds of content that parents wish to prevent their children from seeing. For example, most would agree that it's a good idea to keep vulnerable children from seeing websites that encourage suicide, but care must be taken not to prevent access to websites that may discuss suicide in relation to mental health, if they would be useful to children who need help.

3 Consequences for Website Operators

3.1 Accidental Censorship

No filtering system for the world wide web in all its diversity can be completely accurate all the time. The technology for detecting pornography—even assuming it could be unambiguously defined—or other kinds of content with anything close to 100% reliability simply doesn't exist yet, and isn't likely to for a long time.

So any filtering system will have false positives: websites which are classified as undesirable and blocked because of some accident of the way the filter's algorithms are constructed. For example, I intend to publish a copy of this response on my blog, but since it contains words such as *pornography* it could be misinterpreted by a filter as something more salacious than it is.

This kind of wrongful blocking could have serious consequences for the owner of a website. If a website belonging to a business which has customers in the UK is blocked, they are likely to lose custom. The blocking may even render their business unsustainable. Large businesses will notice a decline in orders and have the legal muscle to get blocking software updated in their favour, but most companies are not in that position.

For websites belonging to individuals and non-profit organisations, the harm caused by blocking would be to prevent them getting their message out to an audience who would otherwise find it useful. This has obvious implications for free speech. It will be especially problematic for websites that provide information or opinions on topics to do with sex, suicide prevention, drugs, etc. For example, websites that provide sex education resources, or advocate political or moral positions on controversial subjects, are more likely than others to be blocked because of the words they will likely use. Such websites are vulnerable to censorship because they usually don't have access to a large technical staff or legal team, and may struggle to convince politicians and the media to take notice of their situation due to the controversial nature of their content.

3.2 Chilling Effects

As people who run websites become more aware of the potential for their properties to be blocked, they may begin to alter their behaviour to compensate. E-commerce businesses selling products on their websites may decide not to stock particular products if they think there's a risk that related words or images could lead to their website being blocked. The damage to a business of being blocked—especially for UK companies which sell mainly to UK customers—would be so great that even the slightest risk of wrongful blocking would be considered unacceptable.

New business ventures may decide to base themselves in other countries or concentrate on selling to other markets to avoid the UK if they see the UK as a place where blocking is more prevalent and carries a higher risk than in other countries.

For non-business websites, a fear of all their content being blocked because of some small part of it may lead to people to refrain from writing what they otherwise would, or being more restrained in how they express themselves. Ridiculous as it may seem, it wouldn't be unprecedented for people to start using euphemisms or made-up slang instead of speaking directly, so as to avoid words that might attract the attention of the filtering software.

Some services that allow user-generated content, such as discussion forums and social networking services, will introduce tighter restrictions on what content users are allowed to post, so as to avoid having their whole service blocked. This would particularly be the case for services aimed at parents, such as Mumsnet.com, since a large proportion of their users would have filtered access.

3.3 Avoiding and Recovering from Blocking

If websites are to steer clear of being blocked by filtering software, they need to know what content is going to trigger the blocks. But as discussed above, there is no definition for what material is to be filtered, and each ISP is likely to block different things.

If a website is accidentally blocked—meaning they haven't done anything wrong, and haven't published any content they would reasonably expect to trigger the filters—then they need to be informed when this filtering is happening. Individuals and small companies running specialist websites are unlikely to notice that some of their visitors are not being shown their website. If they aren't aware of what's happening, then they won't be able to do anything to address it.

If a website is wrongly blocked, then its operators need to be able to resolve that situation. There must be some appeals process that can be used conveniently, and without cost, to have the (probably automatic) decision to block their website reviewed. Requiring them to contact the companies who supply the filtering software would not be enough, since there may be many such companies, there may not be a definitive list of them, and they have no incentive to resolve issues that only affect a handful of people visiting a particular website.

None of these issues are discussed in the consultation, but they need to be considered before any default-on network-level filtering is required of British ISPs.

4 Consequences for Internet Users

4.1 Filtering Applied Per-Connection

If internet access is filtered at the network level, by a household's ISP, then many children will be able to trivially bypass the filtering by borrowing someone else's internet connection. In some cases this could be done simply by taking their laptop or other mobile device to a friend's

house. They are also likely to be able to find unfiltered wireless internet connections. Indeed, even if wifi provided in places like public libraries and coffee shops is filtered, many houses have unintentionally left their wifi routers unsecured, allowing potentially unfiltered access to the internet by more tech-savvy children. Using software instead running on each device that can access websites would avoid these ways of routing around the filtering.

A per-device arrangement would also allow parents more flexibility in accessing the internet unfiltered on their own computers, or by temporarily disabling the filtering software on a shared computer. This would allow parents to keep their own password-protected computer, or to log in to a separate account on the same computer—for which their children didn't know the password—on which the filtering software was disabled. It would also allow parents to allow unfiltered access to older children, or adult offspring living with them.

4.2 Registering with an ISP

The need to register a desire for unfiltered access with an internet service provider presents several potential problems. Firstly, there is the privacy issue. A list of people who don't want their internet access to be filtered is sensitive information, especially if it is misinterpreted—as seems likely—as a list of people who are interested in pornography. We have seen many times in recent years that private information can easily be leaked or stolen, even when held by organisations who one would expect to have the expertise to hold it securely.

As discussed above, it also reduces the flexibility of parents to control *who* in a household should be able to get unfiltered access.

If internet filtering software is chosen and controlled by ISPs, instead of the people who use their services, then people will be less likely to 'shop around' for a filtering solution that suits them. This will reduce competition that would otherwise lead to companies trying to produce higher-quality filtering software, and reduce customer choice. It would also make it easier—and politically tempting—for future governments to impose filtering of specific content they find objectionable.

Finally, network-level filtering may prevent adults in a household from accessing blocked content even if they have decided that they don't want the filtering. Presumably the decision as to whether a house's broadband should be filtered will be made by whichever person orders the connection. Even if there are no children in the house, some people may want

filtered access, but by choosing it for themselves will impose the filtering on other members of the household. People will be reluctant to ask an ISP to remove the filtering if they are concerned about a spouse or other family member finding out and asking awkward questions, and they may have to ask that person directly anyway if they don't know the details the ISP will ask for when contacted.

The person who controls whether the filtering is enabled may be a spouse, an elderly relative, a paid carer, or an adult child who helped get the internet connection set up in the first place. Many adults would prefer not to explain to these people exactly what blocked content they are interested in accessing.

5 Other Solutions

I'm not an expert in helping children use the internet safely, so I'll leave it for others to offer ideas about more positive ways to approach these problems. However, any solution must surely include better computer education for children and parents, and better sex education in schools to prepare children for what they will (sooner or later) find online. Technological solutions can help, but there's no magic bullet.

6 Issues with the Consultation

The consultation is, as it states, directed at parents and the professionals who would be responsible for implementing any filtering system the government chose to require. This ignores the large number of people such as myself who are neither. The council should remember that not everyone who uses the internet is a vulnerable child, or a parent trying to protect a child. A default-on network-level filtering system would affect all of us, not just those the council is concerned for.

In section 3 of the consultation, question 10(a) asks parents whether they'd like to have pornography automatically blocked from being accessed. I think this could be misleading, and may reflect a lack of consideration of the limitations of internet filtering software by the council. No filtering software will be completely effective in blocking *all* pornography, and all filtering software will block at least some things which aren't pornographic. The question may have garnered a different response if it asked whether parents would like to have some (perhaps most) pornography blocked from view, and some other things that aren't objectionable

also blocked as collateral damage.

Finally, the consultation response form itself points out that consultations should normally allow at least 12 weeks for responses. It is claimed that the response period was cut short in this case because of changes to be introduced by October 2012, but surely it would have been better to wait and evaluate the effectiveness of those changes before considering any more.