Why device-based Internet filtering via active choice is the best solution for child-protection online

February 2012. For more information please contact peter@openrightsgroup.org

Internet filtering tools can help parents manage the risks their children face when going online. There are different ways of trying to filter Internet content. The following briefly outlines the benefits and weaknesses of these different methods, with suggestions for the issues that any impact assessment of such filtering should address.

The filtering options

There are three different ways that filtering can work:

1. **'Device-based' filtering** (meaning tools installed on each device, such as a laptop, 'tablet' or mobile phone, tailored to the user of that device)
2. **'Router-based' filtering** (meaning tools installed on the device in a household that delivers their Internet connection).
3. **'ISP-level' filtering** (meaning filtering that is managed by the ISP when they handle Internet traffic).

How it works:

Black- and white-lists: Filtering can be based on either a 'blacklist' or a 'whitelist'. A blacklist is a list of sites that a filtering tool should block. Given the sheer number of websites, blacklists are typically created through some form of automated classification process - and tend to be error prone as a result. A whitelist is a list of sites that a filtering tool should allow the user to see. Whitelists tend to be small and, as a result, well categorised. They are better suited to younger users, but do not 'scale' well.

Device-based blocking works through settings on software such as web browsers or child-protection focused browser apps for mobile devices, and it will usually be possible to configure filtering for individual users of that device. The actual 'filtering' happens on the device itself – meaning the software decides whether to block a particular connection or not at the point when the user wants to visit a site or service.

Router-based blocking. This establishes a filter on the 'box' within the household that delivers the internet connection to a given household. In doing so, it is possible to configure different filtering settings for the different devices that connect to it.

ISP-level blocking. An ISP is a kind of 'middle man' between an Internet user and the rest of the Internet. When a user tries to connect to a website, the ISP is responsible for establishing what the user wants to see, and serving them the right content. It is possible for the ISP to check if the site or service they are trying to connect to corresponds to a blacklist, or does not feature on a white list, and block the attempted connection.

As a rule, the 'closer' to a user the filtering happens, the more control over that filtering is possible.

Benefits and weaknesses of the filtering techniques

1. Device-based filtering allows settings to be set for each device and, potentially, each user of that device, permitting more granular control over what is being filtered. It therefore satisfies the need for control across a number of devices, within and outside the household, which belong to users of different ages and with different needs. It also avoids the technological problems of ISP level filtering, including a 'one size fits all under-18s' approach. Because of the direct relationship between user and the developer of the filtering tool or app, there is an opportunity to support the emergence of responsive solutions to parents' needs. The downside to device-based filtering is that it requires marginally more effort and engagement from parents.

2. Router-based filtering is attractive as it also permits of device-specific filtering, but would not allow for user-specific settings. Problems with this approach include children finding alternative connections within the household (public wifi, for example, or a neighbour's open connection), or devices (for example an iPad) being taken out of the house (for example, to a friend's house) where they are subject to the filtering (or lack of it) available there.

Furthermore, there could be unintended market effects of recommending router-based filtering tools. This will likely mean router manufacturers taking on additional costs to develop filtering software. In turn this may reduce the supply and choice of routers to ISPs (as not all router suppliers will). The cost will likely be passed on to *all* Internet users, not just those who require filtering tools, as ISPs are likely to deploy the same routers to all users.

3. ISP-level filtering is attractive because it promises a simpler 'pressure point' to address the problem – there are fewer ISPs than there are users! However, it is the least attractive from the perspective of wanting to provide granular control, specific to users of devices, as close to the user as possible.

a. ISP-level and router-based filtering share two problems. First, ISP-level filtering is similarly unable to deal with user-specific filtering settings. Second, both are **unable to filter 'https' encrypted traffic**. This means they risk **becoming obsolete** as a mechanism of controlling traffic as 'encryption' is more widely adopted.

'Https' encryption is a way that traffic is made unreadable by 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. Encryption makes it impossible for an ISP to 'check' the 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'.

Device-level blocking still works when encryption is used, however – the device is able to 'see' what page the user is trying to access before the request is encrypted. Put another way, the user can see a website being accessed over an encrypted connection, and so can the browser-based filtering. Furthermore, if there are restrictions on what a user can install on a device, then many of the circumvention techniques will not be possible.

b. There are t**wo additional problems more specific to ISP-level filtering**.

First, using ISP filtering, **control over what is blocked, and why, rests ultimately with ISPs**. This means it is less transparent, with the onus on the ISP to communicate to users what filtering is happening on their networks. There are a number of problems that follow from this issue.

First, ISP-filters can be subject to abuse or exploitation for reasons other than child protection, for commercial or political reasons. Second, it can be harder to manage problems such as mistaken blocking. This is because the ISP acts as a further intermediary between the user and the filtering – an intermediary whose core commercial interest is not accurate filtering. Similarly, as with router-based filtering, it is harder to account for different users in a single household (for example, children of different ages).

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 is potentially gathered by those companies as well.

Active choice, device-based filtering

However it is done, filtering is fallible. It can block access to the 'wrong' content, either through deliberate abuse or by accident. And it can be quite easy to circumvent. Furthermore, evidence shows that the management of the risks young people face online is best done through engagement between parent and child[1]. As a result, the optimal model of internet filtering follows two principles:

1. The choice to have filtering on a connection should involve active, informed consent by the account subscriber (sometimes called an 'active choice').

2. The filtering should happen as 'close' to the person requiring the filtering as possible.

[1] Livingstone et al, 'Risks and Saftey for children on the Internet: the UK report', December 2010