Agenda Item 5c

Net neutrality consultation response

Thank you for the opportunity to respond to Ofcom's consultation on "Traffic management and 'net neutrality'". I am pleased to enclose our response. This response has been prepared jointly by the Internet Watch Foundation and our Funding Council, comprised of member companies from the online sector.

Background

The IWF was established in 1996 by the internet industry to provide the UK internet Hotline for the public and IT professionals to report criminal online content in a secure and confidential way. The Hotline service can be used anonymously to report content within our remit. We work in partnership with the online industry, law enforcement, government, and international partners to minimise the availability of this content, specifically:

- child sexual abuse images hosted anywhere in the world
- criminally obscene adult content hosted in the UK
- incitement to racial hatred content hosted in the UK
- non-photographic child sexual abuse images hosted in the UK.

We are an independent self-regulatory body, funded by the EU and the wider online industry, including internet service providers, mobile operators and manufacturers, content service providers, filtering companies, search providers, trade associations, and the financial sector. Our self-regulatory partnership approach is widely recognised as a model of good practice in combating the abuse of technology for the dissemination of criminal content. Member organisations who support the IWF nominate representatives to a Funding Council. The Funding Council elects three of its members to the IWF Board.

Potentially illegal content

We would like to comment about the principle raised at Figure 1, 2.6 on page 6 of the consultation document.

Some of our Members are Service Providers who block their customers from accidentally stumbling across child sexual abuse content on the Internet as part of a voluntary self-regulatory initiative. Apart from the shocking nature of the content, accessing and or storing the content with the appropriate motive could lead to arrest and possibly prosecution. We should point out that the content is not primarily blocked for the purposes of traffic management, although it is appreciated that traffic management could result from content blocking, but because it is a criminal offence to access such material. This is a distinction that we feel should be highlighted i.e. the difference between the blocking of material the downloading of which is unlawful, for example unlawful downloads of music and copyright issues and that which is criminal, e.g. child sexual abuse images. Therefore, regardless of the outcome of this consultation, we believe many of our UK Service Providers will wish to voluntarily continue this initiative aimed at protecting their customers from child sexual abuse material and therefore we feel this concept should remain a separate debate to that of general traffic management discussions.

Transparency and blocking

We believe that removal at source is an effective method of combating criminal content within our remit and as a result such content has been almost eradicated from being hosted on UK networks. We also work internationally to encourage the removal of child sexual abuse images from the internet by passing details of every identified non-UK website to our partner Hotline in that country so they can investigate it within their own legislation and in cooperation with their national law enforcement agencies.

Whilst child sexual abuse images hosted abroad remain available, the UK internet industry has voluntarily agreed to block access to them using a list provided by the IWF. Blocking is a short-term disruption tactic which may help protect internet users from stumbling across images, whilst processes to have them removed are instigated.

Since 2004 many companies have voluntarily chosen to make use of this list to protect their customers. The list typically contains 500 to 800 URLs at any one time and is updated twice a day to ensure all entries are live.

IWF's role in this blocking initiative is restricted to the compilation and provision of a list: the blocking solution is entirely a matter for the company deploying the list. Our list is designed and provided for blocking specific URLs only. Any decision to convert or adapt the list to block whole domains may lead to the over blocking of legitimate content and is not supported by the IWF.

We have been exploring with our industry partners the use of landing or error pages when access to content on our list is denied by the service provider. As a principle IWF supports transparency about why internet pages containing potentially criminal content have been blocked coupled with the right for a consumer to appeal should they have been prevented from seeing a legitimate page. Simply displaying a "404 page not found" error does not provide any reason to the consumer as to why access has been denied.

Therefore, if any means of blocking were to be used as a wider traffic management initiative, our view is that it is essential for there to be transparency to the consumer at the point at which access is blocked with a reason given as to why access has been denied with an explanation as to what other options the consumer has open to them.