

# Website blocking: submission to Ofcom's technical feasibility assessment

April 2011

In February Secretary of State Jeremy Hunt instructed Ofcom to review whether website blocking by internet service providers (ISPs), as provided for in sections 17 and 18 of the Digital Economy Act 2010, could technically work. The terms of reference for Ofcom's technical feasibility assessment are:

- Is it possible for access to the site to be blocked by internet service providers?
- How robust would such a block be – ie would it have the intended effect, and how easy would it be to circumvent for most site operators?
- What measures might be adopted by internet service providers to prevent such circumvention?
- How granular can blocking be – ie can specific parts of the site be blocked, how precise can this be, and how effective?
- How effective are sections 17 and 18 of the Act in providing for an appropriate method of generating lists of sites to be blocked?
- If possible, identify either a potential range of costs for ISP blocking solutions or the main drivers of those costs.<sup>1</sup>

While Consumer Focus welcomes the opportunity to make a submission to Ofcom to inform its assessment we believe that it would have been beneficial if Ofcom had based its assessment on a public consultation. Sections 17 and 18 have never been publicly consulted on and were made law without any economic impact assessment. Website blocking is a significant public interest issue, particularly in relation to over-blocking and potentially negative consequences for all UK internet users. Therefore we believe that the assessment Ofcom is to provide to the Secretary of State end of this month should be published. Sections 17 and 18 should not be implemented without proper impact assessments and public consultations, and we believe it would be appropriate for the Department for Culture, Media and Sport (dcms) to open the issue of blocking websites that host copyright infringing content to public consultation. Not least because what ought to be the overriding policy question has not yet been answered, ie would website blocking increase consumers' use of legal services and support an innovative and dynamic market in copyrighted content?

Recent moves to examine whether website blocking could effectively be employed to block UK consumers' access to copyright infringing material has been largely inspired by the perceived success of blocking websites hosting child abuse images. The Internet Watch Foundation (IWF) maintains a blacklist for this purpose since 2004, which is used by UK ISPs to block websites using network level address blocking. There are in principal four types of network level address blocking: DNS blocking; web proxy blocking; IP address blocking; and hybrid blocking, or Cleanfeed, which is a combination of IP address blocking and web proxy blocking. The latter is currently used by ISPs to block child abuse images. Other methods of content suppression include 'notice and takedown', network level filtering and end-user filtering. The blocking of websites which host copyright infringing content by ISPs at network level poses three principle risks for UK consumers:

- Degraded internet service, including speed and network reliability, for all UK consumers,
- Increased price of broadband for all
- Denying all consumers access to legal content and services

<sup>1</sup> Ofcom to review aspects of Digital Economy Act, dcms, 1 February 2011

An overriding concern with network level address blocking techniques is ‘over-blocking’ or ‘collateral damage’. Website blocking is a relatively crude and untested technology which may result in the blocking of websites beyond the intended target, negative effects on online services and impact on network performance, particularly speed. There is a significant risk of negative impacts on all internet users – either by denying them access to content that is legal and they have a right to access, or degradation of service. Such chilling effects engage the right to freedom of expression, that is the right to receive and impart information. Any restrictions on the right to freedom of expression must be proportionate and established in law. This means that such restrictions must be precise so as to be reasonably certain and foreseeable, enabling a person affected by the law to regulate their conduct, and provide adequate safeguards against abuse. The chilling effects of website blocking also impact on the rights of internet subscribers to an internet connection of the speed and reliability advertised to them, that enables them to send and receive content of their choice, and use services of their choice. Any scheme to block websites that host copyright infringing material must therefore be effective and proportionate, and the question of whether it is technically possible to only block one website needs to take centre stage in Ofcom’s technical feasibility assessment. Furthermore, we believe that Ofcom, in its technical feasibility analysis, must consider:

- Whether the aim is ‘protection’ or ‘compliance’ blocking, and whether either is technically feasible and effective
- Whether websites or domains are to be blocked, and whether the technology exist to block website without collateral damage such as over-blocking and a negative impact on the relevant online service
- The number of websites to be blocked, to determine which technique of website blocking is technically feasible
- The complexity involved in identifying copyright infringing material. The process of identifying websites that host copyright infringing material cannot be wholly automated, similarly the necessary appeals process cannot be wholly automated
- The likely impact on internet service at network level for all internet users

While we realise that Ofcom’s assessment is narrow in scope and focuses primarily on whether the blocking of websites which host copyright infringing material is technically feasible, we believe Ofcom needs to consider what is realistically possible. As such, cost needs to be a central concern. It would be irrational for Ofcom to advise the Government that the blocking of websites that host copyright infringing content is technically possible, while the cost of implementation and maintenance is so astronomical that it renders website blocking unrealistic in practice. Cost is likely to be a significant issue as the technology required for granular blocking of websites, which avoids collateral damage, tends to be more expensive than other less precise methods.

Legality is another significant factor Ofcom ought to consider. Network level address blocking and network level filtering may not comply with the mere conduit principle as enshrined in the E-Commerce Directive, data protection and privacy laws. The E-Commerce Directive also prohibits the imposition of a general monitoring obligation on ISPs, ie ISPs monitoring the information which they transmit or store, or actively seeking facts or circumstances indicating illegal activity. It is therefore critical that the techniques used for website blocking are themselves legal and Ofcom should advise the Government whether website blocking techniques it has identified as technically feasible are legal under relevant UK and EU law.

### **‘Protection’ and ‘compliance’ website blocking**

In assessing whether the blocking of websites hosting copyright infringing material is technically possible Ofcom must draw a clear distinction between ‘protection’ and ‘compliance’ blocking. Significant technical considerations, such as the method of content suppression, and ultimately the cost–benefit analysis of any proposed scheme will depend on the purpose of the web blocking. We are not aware of any European country that has successfully implemented compliance blocking for child abuse images. It is often overlooked that the IWF emphasises ‘takedown’ of child abuse images and only blocks a relatively small number of websites if takedown fails. The IWF’s primary

success has been in terms of takedown and protection blocking, ie preventing internet users from stumbling across child abuse images. It has been less successful in terms of compliance blocking, ie preventing paedophiles from accessing child abuse images.

In its Annual Report 2010 the IWF clearly states that 'blocking is not a complete solution; it cannot put an end to offenders abusing children nor can it effectively deny determined criminals who are actively seeking such material.' In March this year moves to establish a voluntary scheme to block websites hosting child abuse images in the Netherlands, modelled on the IWF, have come to a halt. Based on a Dutch study and the experience of the IWF Dutch ISPs concluded that blocking websites 'can no longer serve as a reliable and effective way to contribute to fighting child pornography on the internet' and 'therefore cannot be employed effectively'. This conclusion was reached on the basis that in recent years the number of websites hosting child abuse images had significantly declined, and the distribution of child abuse images has shifted to other internet services.<sup>2</sup>

It appears that the blocking of websites that host copyright infringing content could only hope to be protection blocking and as such won't have a significant impact on those users who seek copyright infringing material. Overall Consumer Focus does not believe that website blocking will effectively address online copyright infringement by consumers. Protection blocking does not address the root causes of large-scale online copyright infringement, which is the failure of some industries to satisfy consumer demand with legal online services. This failure is, to a large extent, amplified by overly complex copyright licensing regimes, particularly in relation to online content and cross-border licensing. On a technical level we believe that website blocking is likely to be ineffective because web-based services are not the primary internet service through which consumers access and share copyright infringing content. Non-peer-to-peer filesharing methods of distributing copyright infringing material are already highly fragmented across off-line methods, non-web-based internet services such as internet forums and email, and web-based services such as blogs, video sharing sites and cyberlockers. It is highly likely that the immediate reaction to any blocking of websites would be the accelerated fragmentation and migration towards non-web based service. The importance of web-based services to access and share copyright infringing content is, in any case, likely to be small. We therefore fundamentally question the effectiveness of protection blocking.

### **Differentiating between domain blocking and website blocking**

To date the debate has mainly focused on website blocking, ie the blocking of single URLs, rather than domain blocking. Domain blocking raises significant concerns in relation to over-blocking and therefore raises major freedom of expression issues. Consumer Focus cannot envisage a situation where domain blocking would be proportionate. However, it is technically much more difficult to block websites than domains. IP address blocking and DNS blocking in particular are associated with over-blocking and are likely to be unsuitable for the blocking of websites only. Proxy blocking is considered to be more precise, but potentially expensive. Hybrid blocking, a combination of IP address blocking and web proxy blocking, also known as Cleanfeed, is cheaper than proxy blocking and more granular than IP address blocking. However, hybrid blocking is used to block websites on the IWF blacklist and an attempt by the IWF to block one Wikipedia page for UK consumers resulted in significant unintended collateral damage. When, in December 2008, the IWF blacklisted the Wikipedia page 'Virgin Killer' 95 per cent of UK internet consumers were effectively prevented from contributing to the encyclopaedia because they were all routed through a small number of IP addresses. Whether it is technically possible to block websites without collateral damage in terms of over-blocking or effectively disrupting an online service entirely is particularly relevant in relation to online services hosting user generated content, such as Blogger, YouTube, Flickr, MySpace and Facebook. It would be unacceptable if the blocking of one website prevents practically all UK consumers' from effectively using the service.

---

<sup>2</sup> **Dutch providers abandon 'ineffective' web blocking**, Bits of Freedom, 7 March 2011

## Automatisation of blacklist and appeal process

Website blocking depends on a list of addresses to block. The IWF foundation has established a complex institutional governance framework to supply ISPs with a blacklist, establish the criteria and deal with appeals. In assessing the technical feasibility of blocking websites that host copyright infringing material Ofcom needs to consider whether all or part of this process can be automated. Consumer Focus believes that it is not possible to wholly automate the process whereby websites hosting copyright infringing material are identified. The complexity of copyright, which is licensed on a territorial basis, in the online context, where UK consumers can access websites hosted by servers in other jurisdictions, means that identification of websites which host copyright infringing material is complex. Identifying copyright infringing content with any degree of certainty would involve the assessment of complex licensing agreements across jurisdictions. The likelihood of disputes arising over what is and what is not copyright infringing content is significantly higher than in the case of child abuse images being blocked. Again, we do not believe that the necessary appeals process could be wholly automated.

## Number of websites to be blocked

The number of websites to be blocked as part of any scheme needs to underline Ofcom's analysis of whether the blocking of websites hosting copyright infringing material is feasible. Copyright infringing material is far more prevalent on the web than child abuse images and the IWF blocks a relatively small number of websites; 16,739 across 1,351 domains. The technology employed and maintained to block websites on the IWF blacklist has been developed according to the number of websites that need to be blocked. It is likely that the technology used for IWF blacklist blocking would not cope with larger numbers of websites to be blocked. Equally, any sudden change in the number of websites to be blocked may overload the system. Ofcom's ability to assess the short-term and long-term technical feasibility of blocking websites hosting copyright infringing material therefore depends on the number of websites to be blocked. Furthermore Ofcom must consider the need to update any blacklist of websites that host copyright infringing material. The IWF updates its blacklist twice daily, as websites hosting child abuse images will change address to avoid the block. Effectively the IWF is chasing these websites across the web. Any scheme to block websites hosting copyright infringing material is likely to require the same or higher frequency of blacklist updating.

## Impact on network speed

Website blocking is a technical intervention by ISPs at network level. A key concern of any technical feasibility assessment should be the overall impact on the network, specifically, any degrading of internet service, including speed and network reliability, for all UK internet users. This includes consumers, businesses and public intermediaries such as libraries and universities. Internet subscribers have a right to an internet connection of the speed and reliability advertised to them, that enables them to send and receive content of their choice, and use services of their choice. This is particularly relevant for Ofcom's technical feasibility assessment because those network level address blocking techniques which are more granular, and hence potentially avoid over-blocking and collateral damage, also appear to have a significant impact on the network. Web proxy blocking in particular may reduce network reliability and slow traffic of all internet users. It is difficult to imagine a situation where it would be acceptable to degrade the internet service of all UK internet users for the sake of blocking websites which host copyright infringing content.

For more information please contact Saskia Walzel on 020 7799 7977 or email [saskia.walzel@consumerfocus.org.uk](mailto:saskia.walzel@consumerfocus.org.uk)