“Site Blocking” to reduce online copyright infringement

A review of sections 17 and 18 of the Digital Economy Act

Advice

Date: 27 May 2010

Contents

Section **1**

1. Executive summary

The Secretary of State has asked Ofcom to consider a number of questions related to the blocking of sites to reduce online copyright infringement.

The Secretary of State for Culture, Media and Sport has asked Ofcom to report on certain technical matters relating to sections 17 and 18 of the Digital Economy Act 2010 (DEA). Sections 17 and 18 provide the Secretary of State with the power to grant the Courts the ability to require service providers, including internet service providers (ISPs) and other intermediaries, to prohibit access to sites on the internet that are found to be infringing copyright.

Specifically, we have been asked to consider the following questions:

- Is it possible for internet service providers to block site access?
- Do sections 17 and 18 of the Act provide an effective and appropriate method of generating lists of sites to be blocked?
- How robust would such a block be – in other words, 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?
- Can specific parts of web sites be blocked, how precise can this be, and how effective?

There are several techniques available for blocking access to internet sites

We have focused on four currently-available techniques that ISPs could use within their network infrastructure to block sites (we refer to them as primary techniques).

- **Internet Protocol (IP) address blocking**: modifying ISP network equipment to discard internet traffic destined for the blocked site. An IP address is analogous to a telephone number as it uniquely identifies a device attached to the internet. An example IP address is the Ofcom website 194.33.179.25.
- **Blocking via Domain Name System (DNS) alteration:** changing the ISP service that translates domain names e.g. www.example.com into IP addresses e.g. 192.0.32.10. The ISP DNS server, when blocking, tells the requesting computer or device that the site does not exist or redirects the request to an informational web page, for example one which explains why access to the site has been blocked.
- **Uniform Resource Locator (URL) blocking:** the blocking of specific items, such as web sites or addresses e.g. http://www.example.com/pirate.zip. ISPs already block URLs (supplied by the Internet Watch Foundation) that link to web content relating to child sexual abuse.
- **Packet Inspection:** blocking techniques which examine network traffic either at a high level, (Shallow Packet Inspection (SPI)), or more detailed level (Deep Packet Inspection (DPI)).

We also consider three hybrid options:

1. DNS blocking coupled with shallow packet inspection;
2. DNS blocking coupled with URL blocking; and
3. DNS blocking coupled with deep packet inspection.

We have assessed each of the techniques against seven criteria: speed of implementation; cost; blocking effectiveness; difficulty of circumvention; ease of administrative or judicial process; the integrity of network performance; and the impact of the block on legitimate services. A summary of our findings is illustrated below in Tables 1 and 2.

Table 1: Summary findings: primary techniques

	Assessment Criteria						
Blocking technique	Speed of implementation	Cost	Blocking effectiveness	Difficulty of circumvention	Ease of administrative or judicial process	Integrity of network performance	Impact on legitimate services / law abiding consumers
IP address	✓✓	✓✓✓	✓	✓	✓	✓✓	✓
DNS*	✓✓✓	✓✓✓	✓✓✓	✓	✓✓✓	✓✓✓	✓
Shallow Packet Inspection	✓✓	✓✓✓	✓	✓	✓	✓	✓
Deep Packet Inspection	✓	✓	✓✓✓	✓✓	✓✓✓	✓	✓✓✓
URL	✓✓	✓✓	✓✓	✓✓	✓✓✓	✓✓	✓✓✓

✓ = Worst ✓✓✓ = Best

* The attractiveness of DNS-blocking could be diminished in the longer term following the implementation of DNS Security Extensions (DNSSEC), a technology used to authenticate and verify domain name queries to reduce incidences of fraud online (through malicious sites). This is discussed further below.

Hybrid options could potentially be used to improve the robustness of blocking, principally by increasing the complexity of circumvention. These are reviewed below.

Table 2: Summary of findings: hybrid of blocking techniques

	Assessment criteria						
Blocking technique	Speed of implementation	Cost	Blocking effectiveness	Difficulty of circumvention	Compatibility with judicial process	Integrity of network performance	Impact on legitimate services / law abiding consumers
Hybrid: DNS* & URL	✓✓	✓✓	✓✓	✓✓	✓✓✓	✓✓	✓✓
Hybrid: DNS* & SPI	✓✓	✓✓	✓	✓✓	✓✓✓	✓✓	✓✓
Hybrid: DNS* & DPI	✓	✓	✓✓✓	✓✓	✓✓✓	✓✓	✓✓

✓ = Worst ✓✓✓ = Best

* The attractiveness of DNS-blocking could be diminished in the longer term following the implementation of DNS Security Extensions (DNSSEC), a technology used to authenticate and verify domain name queries to reduce incidences of fraud online (through malicious sites). This is discussed further below.

None of these techniques is 100% effective; each carries different costs and has a different impact on network performance and the risk of over- blocking.

We believe that it is feasible to constrain access to prohibited locations on the internet using one or more of the primary or hybrid techniques. The approaches considered vary in how precise they are,

their operational complexity, and therefore their effectiveness. None of the methods will be 100% effective.

We find that there is no uniformly superior technique as each carries risks in different areas. For instance IP address blocking carries a risk of over blocking, whilst URL blocking is limited in the scope of content it can block effectively. Over-blocking occurs where a block is imprecise, so legitimate content is blocked alongside infringing content.

If blocking is to be implemented, we consider DNS blocking to be the technique which could be implemented with least delay. While it carries a risk of over blocking, since it blocks at the level of the domain (blocking all websites in the blocked domain, when only one may have been infringing), it would be quick to implement, as existing systems could be easily adapted, and would appear to require only fairly modest incremental investment for service providers. Blocking could be made more robust where DNS blocking was complemented with URL blocking or DPI.

However, DNS blocking may be of more-limited value in the longer term. The implementation of DNS Security Extensions (DNSSEC), a technology used to authenticate and verify domain name queries to reduce incidences of fraud online (through malicious sites), is likely to be incompatible with DNS blocking. DNS-blocking could still be used to block sites identified as infringing copyright even after DNSSEC has been rolled out. However, under DNSSEC users attempting to access a blocked site would no longer be re-directed to an alternative webpage and so would be unable to tell between a lawful court sanction blocking action and malicious activity on their DNS query. We would expect DNSSEC to have been widely deployed in the UK within the next three to five years.

For a longer-term solution, a packet inspection based approach would be the most effective technique, based on our knowledge of currently available technologies. However, it is the most technically complicated and expensive technique to deploy and there are a number of legal questions which would have to be addressed, such as the compatibility of DPI blocking with laws on privacy, data protection and communications interception. Additionally, DPI may affect the performance of networks, as each and every network packet is inspected to indentify infringing traffic.

We are sceptical that IP address blocking is a sufficiently precise or robust method of site blocking to be considered for deployment either as a primary or a secondary technique. The use of IP address blocking carries a significant risk of over-blocking given that it is common practice for multiple discrete sites to share a single IP address. Estimates vary on the scale of IP address sharing between websites; a 2002 study estimated that 87% of websites shared an IP address within active COM, NET, and ORG web sites.[1] In addition, circumvention is technically trivial for those site operators who wish to do so, for example by changing IP addresses.

URL blocking, whilst granular and straightforward for most ISPs to deploy, is of limited value as it is effective only against web traffic.[2] This would create a risk that infringement would simply migrate from web traffic to other means of distribution, such as Newsgroups or file transfer protocol (FTP).

All techniques can be circumvented to some degree by users and site owners who are willing to make the additional effort.

For all blocking methods circumvention by site operators and internet users is technically possible and would be relatively straightforward by determined users. Techniques are available for tackling circumvention, but these are of limited value against sophisticated tools, such as encrypted virtual private networks (VPN).

[1] Web Sites Sharing IP Addresses: Prevalence and Significance, http://cyber.law.harvard.edu/archived_content/people/edelman/ip-sharing/ Benjamin Edelman - Berkman Center for Internet & Society - Harvard Law School (September 2003).

[2] We are not aware of any available URL blocking solution which is effective against other URL based internet service.

Nevertheless, site blocking could contribute to an overall reduction in online copyright infringement – especially if it forms part of a broader package of measures to tackle infringement.

Just because it is technically possible for site operators and end users to circumvent blocking, it does not mean that in practice they will universally do so. The extent to which consumers and site operators will seek to circumvent blocking depends on a wide range of factors. These include the convenience and prevalence of circumvention techniques, the relative attractiveness of legal alternatives (and the opportunity cost of the illegal service foregone) and also the ease and efficacy with which site operators can interact with the legal process should they dispute a block.

Although imperfect and technically challenging, site blocking could nevertheless raise the costs and undermine the viability of at least some infringing sites, while also introducing barriers for users wishing to infringe. Site blocking is likely to deter casual and unintentional infringers and by requiring some degree of active circumvention raise the threshold even for determined infringers.

The location of infringing sites can be changed relatively easily in response to site blocking measures, therefore site blocking can only make a contribution if the process is predictable, low cost and fast to implement.

To be effective, copyright owners need to have a practical way of triggering a site blocking procedure. In particular, copyright owners have told us they need:

- **Timely and flexible implementation of blocks**: copyright owners said that to be effective the framework enabled under sections 17 and 18 would have to be capable of putting blocks in place within hours of an application being made. They explained that for live sporting events and for pre-release movies and music, as well as for software, there is a limited window to act before much of the potential benefit of blocks would be lost;

- **A low cost process**: for the process to be accessible to all copyright owners it would need to be relatively inexpensive for them to use. The cost of seeking a blocking injunction under existing legislation is, say the copyright holders, prohibitive for all but the largest copyright owners; and

- **A predictable outcome**: clarity is needed on issues such as the standards of evidence required to secure an injunction and on the responsibilities of a copyright owner to make available content through lawful means. Some copyright owners cite the lack of clarity in the Copyright, Designs and Patents Act 1988 (CDPA) as one reason why only two applications have been made for injunctions under that Act.

We do not consider that sections 17 and 18 would be effective for generating lists of sites to be blocked

We do not think that sections 17 and 18 of the Act would meet the requirements of the copyright owners, as set out above. Specifically, we do not think that using the DEA would sufficiently speed up the process of securing a blocking injunction, when compared to using section 97A of the Copyright Designs and Patents Act, which already provides a route to securing blocking injunctions. As a consequence we are sceptical as to whether copyright owners would make sufficient use of any new process.

We have identified a number of features that a site blocking regime would need to have to increase the likelihood of success.

Consideration should be given to features that would enhance the likelihood of success:

- **Identification of site operators:** Section 17(6) of the DEA requires any application for an injunction to be notified to ISPs and site owners. The normal approach to identify site owners would be to inspect the WHOIS database, the primary source of information on domain ownership. Available research suggests that only 28% of entries in the WHOIS database are wholly accurate and that only 46% of domain owners could be contacted directly or through

indirect means.[3] An effective regime would need to ensure accurate identification, or allow blocking without identification where a site owner was deemed to have not taken sufficient action to allow easy identification and best endeavours efforts had been made to identify them;

- **Timely implementation of a block:** once an injunction has been granted it would appear that it could take days for the block to be put in place by smaller service providers, depending on the blocking technique employed and the network change control regime employed by the ISP. However, it could be done much more speedily (potentially within minutes) where the processes are wholly automated and the ISPs have the appropriate change control processes in place;

- **Granular blocking:** the limited granularity of several of the techniques we reviewed means that there is a risk that a block could inadvertently constrain access to legitimate services, with adverse consequences for those services as well as end users. Consideration could be given to the interaction of "notice and take down" procedures with techniques that over-block. Highly granular blocking is more effective if carried out by site owners. One option would be for site owners to be asked to remove infringing content with site blocking reserved primarily for sites that fail to cooperate in a timely way with "notice and take down" procedures; and

- **Liability of service providers:** If the system of site blocking is to be effective, ISPs will need to be protected from any liability that may arise should over-blocking occur as a result of implementing an injunction.

To be successful, any process also needs to acknowledge and seek to address concerns from citizens and legitimate users, for example that site blocking could ultimately have an adverse impact on privacy and freedom of expression.

Any process designed to generate a blocking injunction also needs to be fair, such that the legitimate interests of other interested parties (i.e. sites which could be blocked by these processes, the end users who may lose access to particular content and the ISPs who may be involved in blocking obligations) can be properly considered by a Court.

The technical ease of circumvention places a particular burden on the process. Where site operators or end users have little faith in the fairness of the process, they will have a stronger incentive to choose to circumvent any block, as opposed to participating fully in the legal process. For a process to be fair then it should satisfy the following principles:

- **Accessibility**: relevant site operators, ISPs and end users would be provided with a fair opportunity to engage with the legal process following the application for a blocking injunction, making representation to the Court as either defendants or interested parties (best endeavours to contact the site operator);

- **Proportionality**: the Court should be satisfied that the granting of a blocking injunction is an objectively justified measure, given the impact of the infringing behaviour on the copyright owner who has made the application. We note that the DEA requires that the Court consider the impact of a block on freedom of expression;

- **Clarity**: it is important that any obligations placed upon service providers to block access to relevant sites are set out clearly. This may include the duration and scope of any injunction, how the costs of any measures should be apportioned and the techniques which the service provider should deploy; and

[3] Draft Report for the Study of the Accuracy of WHOIS Registrant Contact Information http://www.icann.org/en/compliance/reports/whois-accuracy-study-17jan10-en.pdf (17/01/2010)

- **Transparency**: where an injunction has been granted and the block has been implemented there must be some means of informing site operators and end users of the reasons for the site no longer being accessible (i.e. that a UK Court has ordered it be blocked on the grounds that it has infringed copyright law) and setting out clearly what steps they can take to appeal against the injunction.

If there remains a concern regarding circumvention by more determined users, consideration would need to be given to action targeted at third parties that facilitate circumvention, such as VPN providers and search and index sites.

There are complementary administrative measures which, if deployed alongside site blocking, would strengthen its effectiveness. We identify several such measures which are used for impeding or blocking site access. These include domain seizures, use of notice and take down, and search engine de-listing. Whilst these measures may have a stand-alone role to play there are benefits in such measures being pursued as a complement to site blocking.

For instance, an effective notice and take down scheme could be used to provide site operators with an opportunity (and incentive) to remove infringing content, with the threat being that a block will otherwise be implemented. Given the risk of over blocking inherent in the deployment of any of the techniques considered, a system of prior notice would help to protect the legitimate interests of site operators whose sites might otherwise be inadvertently blocked. However, it would represent an additional hurdle in relation to sites offering exclusively illegal content.

Even if a site blocking process is established that can take down the existing location of an infringing site quickly, the operator can relatively easily re-establish the site on a different IP address, URL or domain and the new site can then be "re-found" through a simple search. The impact of taking down a particular location can therefore be compromised. If, on the other hand, a particular location can be removed through site blocking and users cannot easily and quickly find the new location (because of de-listing in search engines) then there would be a significant additional cost of doing business for the operator of the infringing site.

We note that a Bill has been introduced in the US proposing a range of complementary enforcement measures similar to those we identify.[4] The purpose of the Bill is to provide US government agencies and copyright owners with a richer set of tools with which to tackle infringing sites. We consider that there is merit in exploring the role that such measures could play to enhance the effectiveness of site blocking.

Consideration could also be given to ensure the cooperation of VPN providers to secure the blocking of infringing sites. VPN providers could be asked to assist with blocking infringing sites accessed by their customers. Those that do not take part in a scheme could, in turn, find their own service at risk from blocking provisions. However, such a scheme would constitute a significant further escalation, and would therefore require very careful analysis and consideration.

[4] Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011 http://leahy.senate.gov/imo/media/doc/BillText-PROTECTIPAct.pdf

Section 2

2. Introduction

This section acts as an introduction to the subsequent analysis in the report. It begins by outlining why we have undertaken this work (section 2.1), before looking at the existing landscape for the distribution of content online (section 2.2).

2.1 Purpose of the Report

The UK Government has for some time shared the view of many in the creative industries that online copyright infringement is a material concern, a barrier to the growth of the UK's creative economy and that existing measures available to copyright owners were simply not effective. In December 2005, the Chancellor of the Exchequer asked Andrew Gowers to conduct an independent review into the UK Intellectual Property Framework. The Review was published on 6 December 2006.[5]

Gowers recognised the potential value of an industry-led approach and was keen for that to succeed. However, his view was that in the event of the failure of the discussions which were taking place at that time the Government should consider whether there was a role for legislation to require greater cooperation between copyright owners and ISPs over measures to reduce online copyright infringement. This is set out in one of his recommendations, below:

> Recommendation 39: *Observe the industry agreement of protocols for sharing data between ISPs and rights holders to remove and disbar users engaged in 'piracy'. If this has not proved operationally successful by the end of 2007, Government should consider whether to legislate*.

Concerns about standards of evidence required for disconnecting a subscriber, service provider liability, the apportionment of costs and the governance arrangements of any scheme proved to be impossible for the voluntary initiative to resolve.

In the knowledge that a self-regulatory approach had not provided a solution the Government introduced legislation aimed at addressing the issue of online copyright infringement. The Digital Economy Act (DEA) received Royal Assent in April 2010.[6] It includes a number of provisions intended to reduce online copyright infringement; among these, sections 17 and 18 of the Act are intended to facilitate a *site blocking* scheme under which intermediaries (e.g. ISPs) would be required to restrict their users' access to "locations on the internet".

Sections 17 and 18 create a power for the Secretary of State to introduce regulations which facilitate the issuance of "blocking injunctions", as described below:

> "*about the granting by a Court of a blocking injunction in respect of a location*[7] *on the internet which the Court is satisfied has been, is being or*

[5] Gowers Review of Intellectual Property - November 2006
http://webarchive.nationalarchives.gov.uk/+/http://www.hm-treasury.gov.uk/d/pbr06_gowers_report_755.pdf

[6] http://www.opsi.gov.uk/acts/acts2010/ukpga_20100024_en_1

[7] For the purpose of this review we have interpreted location as being internet connected hosts which are capable of a network connection and data transfer to other internet hosts. The internet host may not have assigned a fully qualified Domain Name System name e.g. **www.example.com** and therefore access and connection is via IP addresses only. Similarly a location may be comprised of a number of IP addresses but all resolving to the same fully qualified domain name.

is likely to be used for or in connection with an activity that infringes copyright" (DEA Section 17 (1))

The Secretary of State has asked Ofcom to review the potential efficacy of the site-blocking provisions of the DEA, answering the following questions:

- Is it possible for access to a site to be blocked by internet service providers?
- How effective are sections 17 and 18 of the Act in providing for an appropriate method of generating lists of sites to be blocked?
- How robust would such a block be – in other words 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 – i.e. can specific parts of the site be blocked, how precise can this be, and how effective?

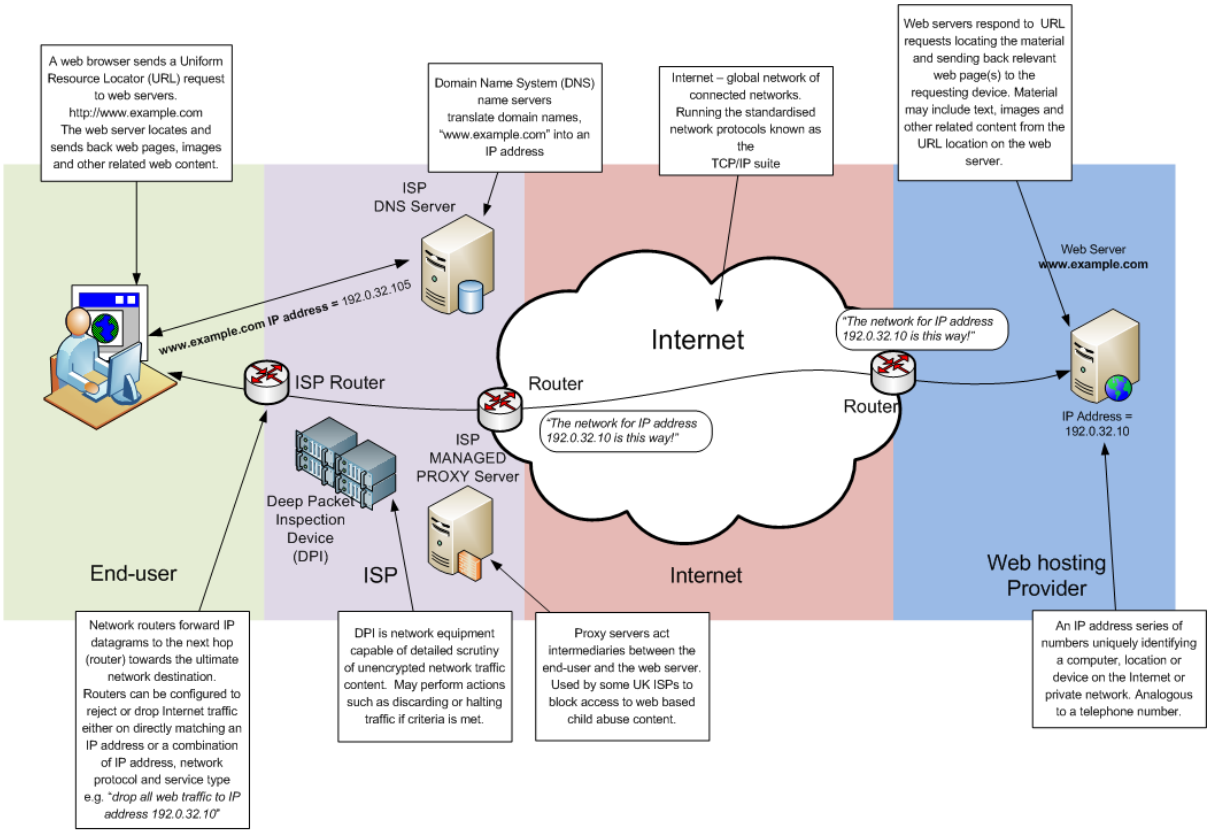
In addition, we have been asked, where possible, to identify either a potential range of costs for ISP blocking solutions or the main drivers of those costs.

This report seeks to answer these questions; but it is also important to note that the report is limited in its scope. We have been asked to provide primarily a technical review of the measures which would be available should the provisions under sections 17 and 18 be enacted. We also consider the likely effectiveness of a framework enabled by sections 17 and 18 to generate lists of sites for blocking and we briefly compare the blocking provisions in the DEA with those which are currently available to copyright owners under the Copyright, Designs and Patents Act 1988.

We do not consider the proportionality of the introduction of site blocking or whether in practice successful actions to secure injunctions could be brought; this will depend both on the evidence and circumstances of specific cases, and on the definitions and procedures which would be laid out in the implementing regulations. These are issues for the Secretary of State, to be addressed as part of the consultative and Parliamentary processes laid out in section 18 of the Act, and for the Courts.

Figure 1 below provides a high-level illustration of the internet, showing how a request from a user to access a site on the internet leads to the information from that site being delivered back to the user. It also provides an introduction and brief explanation of some key terms which are used commonly throughout the report.

Figure 1: Site blocking – key terms



The rest of this section provides an overview of the existing framework for online content distribution, which provides context for the sections which follow.

2.2 The online content landscape

The internet offers an attractive platform for the distribution of content and applications, such as electronic books, films, newspapers and music. It has already transformed the media and entertainment sectors, providing consumers with new and ever more flexible means of accessing, producing and sharing content, creating opportunities for new service providers, such as Spotify and We7, and the potential for new revenue streams, such as subscription and advertising.

Legitimate online services

Consumers can access digital content via the fixed line internet, as well as via mobile devices, and can opt for advertising funded, subscription or pay-per-download services. The British Recorded Music Industry (BPI) currently more than 70 services through which consumers can lawfully access music services, either for streaming or downloading. Music downloading continues to grow, with the BPI reporting that over 21 million albums were bought digitally in 2010, representing 17.5% of album sales.[8] The UK Film Council reports that online film revenues increased from 2008 to 2009 by 156% to £15.9 million and that there are now 32 internet and television-based Video on Demand (VoD) film services available to UK consumers, a five-fold increase in two years.[9] However, digital distribution of film continues to be a small market, relative to more established release windows, such as pay TV and cinema. The internet has also begun to have a transformative impact on book publishing and distribution. In January 2011 Amazon announced that electronic books (or e-books) for its Kindle

[8] BPI MUSIC SALES DIP FURTHER IN 2010 BUT DIGITAL ALBUMS HIT THE MAINSTREAM http://www.bpi.co.uk/assets/files/BPI%20news%20release%20-%202010%20music%20sales%20volumes%20-%205%20Jan%202011%20final.pdf

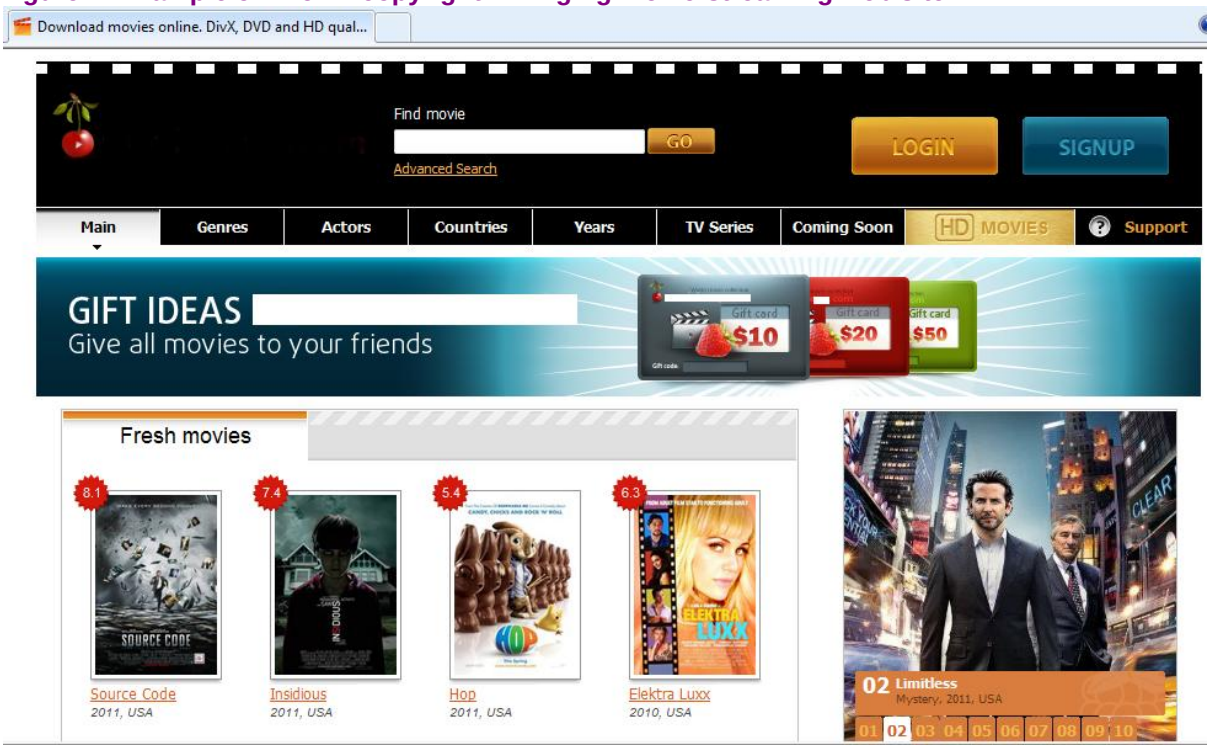
[9] UK Film Council - Statistical Yearbook 2010 - http://sy10.ukfilmcouncil.ry.com/12.0.asp

reader had overtaken sales of paperback as the most popular format on Amazon.com.[10] It is likely that the effects are being felt similarly across other sectors of the creative economy.

Infringing services

As consumer demand for easy access to attractive content across a range of digital devices grows, so does the challenge for the creative industries seeking to capitalise on this demand. Lawful services must compete with those which enable consumers to share, to distribute and to access (often high quality) content unlawfully. Many such services charge consumers monthly subscriptions, are well designed and difficult to distinguish from their lawful rivals.

Figure 2: Example of known copyright infringing movie-streaming web site



Source: Ofcom

As consumers may also be able to access content before it is available via legitimate online retailers (or even before it is available through ***any*** legitimate retailer) the attraction of unlicensed services is obvious. The inability to easily move content between devices, the price levels and the limited range of available content are cited by consumers as additional disincentives to use lawful services.

The lack of high profile enforcement action against those who infringe copyright means that many infringers see little risk of being caught and in any case may not consider what they are doing to be morally wrong (even where they understand that their behaviour is potentially unlawful). Despite the growth in usage of lawful services, it appears that for many consumers copyright infringement remains socially acceptable.

Sites and services offering infringing access to copyright content use a range of technologies. The main techniques currently used to share content unlawfully are listed below:

- **Peer-to-peer (P2P):** decentralised file-sharing systems used for distributing data. P2P technology is used extensively for unauthorised distribution of copyright material such as music, computer software and films. Notable examples of this technology are BitTorrent and FrostWire. Infringing P2P activity may rely on a web server to track the distribution and availability of shared files. Web based searchable indexes of available material on P2P networks are commonplace. P2P technology is also emerging as a distribution mechanism for

[10] http://phx.corporate-ir.net/phoenix.zhtml?c=176060&p=irol-newsArticle&ID=1521090&highlight&ref=tsm_1_tw_kin_prearn_20110127

(lawful) video and web page content via Content Distribution Networks (CDNs), where computers placed at particular points across a network provide local caches for content, reducing the time taken for the content requested to be delivered to the end user.

- **Streaming**: video streaming is an everyday technology used on the internet by many lawful sites, for example YouTube and BBC iPlayer. Video streaming is often incorporated into web pages via technology like Adobe® Flash® Player. Alternatively, a video stream can be viewed via a standalone application such a Real Player® or Microsoft Windows® Media Player. There are illicit websites and internet services that stream, often for payment, unauthorised copies of copyright content such as movies, sporting events and television programmes. P2P streaming, where an end user starts a stream by using an application and viewers receive and share the signal/data with other viewers, is also an emergent method of watching infringing content online.

- **Cyberlockers/Cloud storage**: so called "one-click" hosting requires little technical expertise to use, characterised by a very simple web based upload or download process. Cyberlockers allow consumers to upload files to a web server. A web link to the stored file is created after upload, the link can be shared via posting on discussion forums or the uploader can choose to keep the files private. Cyberlocker/one-click hosting sites are frequently indexed by dedicated search facilities allowing the easy search and location of both legitimate and illicit material. There are lawful uses of this technology such as the backup of personal files such as photographs and documents. Some one-click hosting providers incentivise uploaders by offering financial rewards to popular download links. Downloaders can pay for increased performance, i.e. faster download speeds or to increase the number of files downloaded at once. Copyright infringing uses of this technology include the unlawful download of films, music and software. To further decrease download times and for end-user convenience the uploaded files are frequently stored as a compressed "zipped" archive file format.

- **Newsgroups**: USENET or Newsgroups is analogous to a virtual bulletin board where users post comments and files for reading or download by other subscribers. Newsgroups are organised around common themes and follow a hierarchical structure. Considered a legacy technology, there are subscription News services that offer extensive retention of postings. Newsgroups can be used for the unlawful sharing of copyright content.

Tackling infringing services

The issue of how to tackle the use of such services for infringing activities is complex. These technologies (indeed, many of the same services) are also used for legitimate purposes since they are highly efficient ways of distributing and storing data, content and applications. Some of the most widely known lawful internet services, such as the Spotify music service and Skype's voice over internet protocol (VoIP) product, employ peer-to-peer technology, whilst Amazon has recently announced the launch of a cloud-based music service.[11]

There are already a number of legal, voluntary and administrative approaches to tackling infringing services. A detailed analysis of these measures is outside the scope of our remit, but it is appropriate to draw attention to the range of approaches currently available.

- **Blocking injunctions:** section 97A of the Copyright Designs and Patents Act 1988 (CDPA) gives the Court power to grant an injunction against a service provider *"where that service provider has actual knowledge of another person using their service to infringe copyright."* Such an injunction exists in addition to the power of the Court to grant an injunction in the context of an action for breach of copyright by a particular person.

  We are not aware of any injunction being granted under section 97A. Copyright owners have made us aware of only two applications for such an injunction by them. In the case of

[11] News Release - Introducing Amazon Cloud Drive, Amazon Cloud Player for Web, and Amazon Cloud Player for Android (29/03/11) - http://phx.corporate-ir.net/phoenix.zhtml?c=176060&p=irol-newsArticle&ID=1543596&highlight=

Newzbin[12] the Court refused to grant the injunction to block the site, despite finding that the site was guilty of secondary infringement. The judge refused to grant the broader injunction on the grounds that the application would have applied to rights which the applicants themselves did not own and that Newzbin could not have known about all the infringements taking place through its service.[13] We understand that a further application in respect of Newzbin2 is expected to be heard in July 2011. A brief comparison of section 97A of the CDPA and sections 17 and 18 of the DEA is provided in Section 5.

- **Notice and take-down:** where content is hosted in the UK copyright owners may ask the hosting service provider to take down the content at source. Where this happens the service provider can review the material and take its own view as to whether the content is infringing. YouTube offers a particularly interesting model of this. Where copyright owners identify content which they believe to be infringing, YouTube offers them tools to allow for the content to be taken down or actually monetised. The copyright owner can take a share of the advertising revenue on the page or use the page to promote the copyright owner's own videos on YouTube. If the service provider chooses to remove the content then the party who has posted the content will typically be informed and given the opportunity to challenge the decision, with access to the content being re-instated if the service provider is persuaded that it is not infringing.

  Under US law, there is a formal legal process for such a scheme, operated under the Digital Millennium Copyright Act (DMCA). Service providers are provided with a safe-harbour, which grants them immunity from prosecution (under secondary infringement rules) where they operate within a specific framework in considering requests from copyright owners to block access to sites or to remove content where they are hosting it. We understand that the notice and take down scheme operated by YouTube in the UK is similar to that which it operates in the US, but without the safe harbour protections. Service providers have argued in favour of a similar safe harbour protection being of value in the UK, but have said that European copyright law contains no provision which would allow it.

  A notice and take-down scheme could provide a valuable complement to a technical blocking measure, essentially offering the service provider the opportunity to remove the content in question prior to a formal block being put in place. The opportunity for the site operator to remove infringing content ahead of a block being implemented could be helpful where the blocking technique carried a risk of over blocking. In this context, it is worth noting that the Italian communications regulator (AGCOM) is consulting on proposals for regulated notice and take-down scheme under which the regulator would have powers to require service providers to remove infringing content. That the removal of content was at the request of the regulator would, we assume, protect the service provider from liability.

- **De-listing from search index**: some search engines, most notably Google, will de-list particular sites following the submission of evidence from a copyright owner that the site is infringing copyright. Application to de-list is submitted to Google via post or fax. Google will attempt to contact the site hosting the alleged infringing content and provide them with an opportunity to engage in the process before Google reaches its decision. De-listing can be an effective measure in so far as it makes it more difficult for users to find unlawful sites and it makes it easier to locate lawful alternatives, as they will appear higher on the search rankings than would otherwise be the case.

  De-listing of infringing sites could increase the effectiveness of a blocking scheme. Whilst the operator of a site which has been blocked can move the site to an alternative IP address, URL or domain, if it cannot secure a listing for the new location on search engines then it will prove harder for users to find it and for the operator to effectively re-build its business.

[12] For further background see http://news.bbc.co.uk/1/hi/8594568.stm.

[13] Film industry seeks BT blocking order in Newzbin2 piracy case - http://www.guardian.co.uk/technology/2010/dec/16/mpa-bt-newzbin2

- **Squeeze revenues:** infringing sites can often appear legitimate to users and some are alleged to be successful at generating significant revenues.[14] Some infringing sites charge a subscription fee, carry banner advertising for legitimate brands and often look more attractive to consumers than their lawful alternatives. It can be difficult for a consumer to know whether the site is indeed infringing. Many brand owners are unaware that their adverts are appearing on such sites until it is brought to their attention by copyright owners. Copyright owners have reported some success in persuading those brands to instruct their advertising agencies to withdraw ads from such sites. Similarly, credit card companies are reported by copyright owners as having been put under pressure to withdraw payment platform services from such sites. In addition to helping make the service appear less legitimate, the removal of payment platform services and advertising may make such sites less attractive to operate given the costs of bandwidth and storage required for operation, as well as the inconvenience caused by the disruption and from having to secure alternative payment platform services.

- **Domain seizures:** a recent development in the U.S. has been the seizure of websites which were allegedly illegally streaming live content. In February, the U.S. Immigration and Customs and Enforcement (ICE) department executed a federal Court order in the Southern District of New York, seizing 10 websites.[15] The websites were streaming coverage of National Football League, National Basketball Association and National Hockey League events. ICE has said publicly that further seizures will occur.[16] Visitors to those sites were redirected to a banner advising that the domain name had been seized by the New York office of ICE because of criminal copyright violations. There may be a greater attraction to domain seizures in the US than would be the case in the UK, given that there are more significant domain registries with the US jurisdiction. We believe that such a measure, if implemented in the UK, would only be capable of a limited effect, given that it would only affect domains using ".uk" country code top-level domains. Site operators can respond to a seizure by registering their site in a different country. Whilst this is an inconvenience, it is not a significant barrier to the operation of unlawful sites. The approach could be made more effective through improved international cooperation amongst enforcement agencies, limiting the number of countries to which those subject to seizure orders can switch.

We believe that the measures outlined above could potentially play a role in support of a site blocking scheme, complementing the more technical approaches and, in some cases, helping to compensate for weaknesses inherent in the blocking techniques. A bill has been introduced in the US which would see many of these measures adopted to help the enforcement agencies and copyright owners to tackle infringing web sites based outside of the US.[17] It is too early to predict the outcome for that proposal, but we believe there is value in considering further how such measures could be deployed to enhance the effectiveness of site blocking within the UK.

2.3 The structure of the report

Following this introductory section the report is structured as follows.

- **Section 3 – Understanding how the internet operates:** this provides a brief overview of relevant operational characteristics of the internet and key aspects of its governance and administration.

---

[14] Prosecutors in the case of The Pirate Bay alleged that the site was making more than $1.5m per year from the sale of banner advertising space. This claim was denied by The Pirate Bay. Sundberg, Sam (2 March 2009). ""TPB har tjänat tio miljoner om året"" (in Swedish) (blog).

[15] http://www.ice.gov/news/releases/1102/110202newyork.htm

[16] Reported at http://www.tgdaily.com/business-and-law-features/55249-ice-vows-to-continue-domain-name-seizures

[17] Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011 http://leahy.senate.gov/imo/media/doc/BillText-PROTECTIPAct.pdf

- **Section 4 - Site blocking:** this looks in turn at each of the main site blocking techniques (blocking by IP address, DNS, URLs, Packet Inspection). As well as the basics of each technique, it considers for each one its robustness, responses to possible countermeasures, granularity and other considerations. The section concludes by examining the emerging technological developments that may have a bearing on site blocking.

- **Section 5 – The effectiveness of Section 17 & 18 of the DEA**: in this section we comment on what would be required to be implemented under section 17 & 18 for the framework to be effective at generating lists of locations to be blocked by service providers.

- **Section 6** - **Conclusion**

Section 3.

3. Understanding how the internet operates

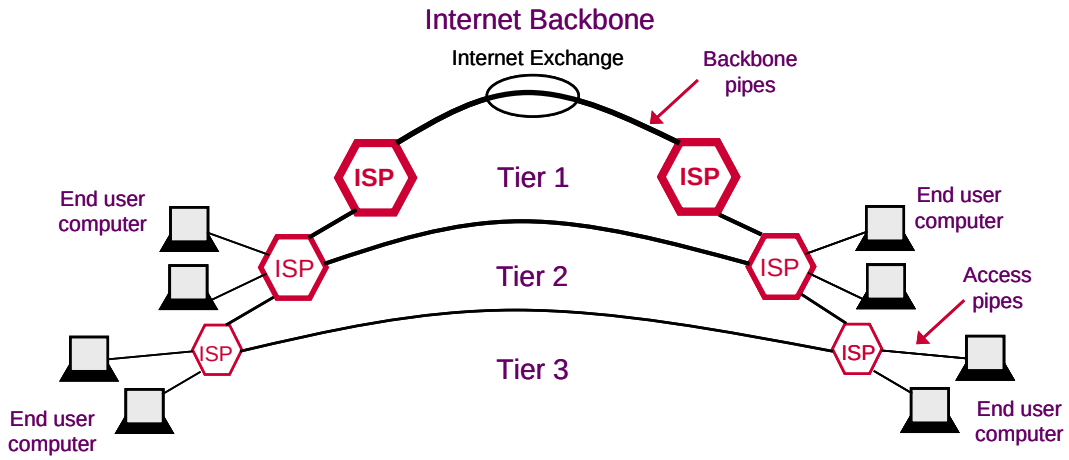
3.1 Introduction

A basic understanding of the how the internet operates is important for any consideration of the different techniques available for impeding access to copyright infringing sites. This section provides a brief overview of the architecture, protocols and governance of the internet, and highlights relevant implications for how a site blocking framework might operate.

The internet's origins date back to the late 1960s with the development of ARPANET, a US defence project which led to the first operational packet switching network. During the 1970s the US Department of Defence involvement receded and over time more US universities, other public institutions and finally commercial communication providers took leading roles, shaping the internet into the global network we are familiar with today.

Internet Service Providers (ISPs) – the network operators which provide end users with access to the internet – largely work in a hierarchical architecture, illustrated in Figure 3. There are three tiers of ISP, each of which will typically have peering (i.e. traffic is exchanged without payment) and paid-for links with other ISPs. ISPs in the same tier peer with one another - exchanging data between each other's customers freely and for mutual benefit. ISPs in the higher tiers sell internet connectivity to those in the tier below. Those in tier one are the major telecom companies and generally do not pay other operators for traffic sent across those other networks (i.e. they operate peering). Tier two operators will peer with some networks (usually other tier two operators), but will also purchase IP transit and other services, typically from tier one operators, to reach the internet. Those in tier three will typically purchase all necessary services from either tier one or tier two operators.

Figure 3: Schematic overview of the internet



Source: Ofcom

The internet is network of globally connected networks that communicate using a standardised set of rules, or protocol suite, referred to as Transmission Control Protocol and Internet Protocol (TCP/IP) stack.

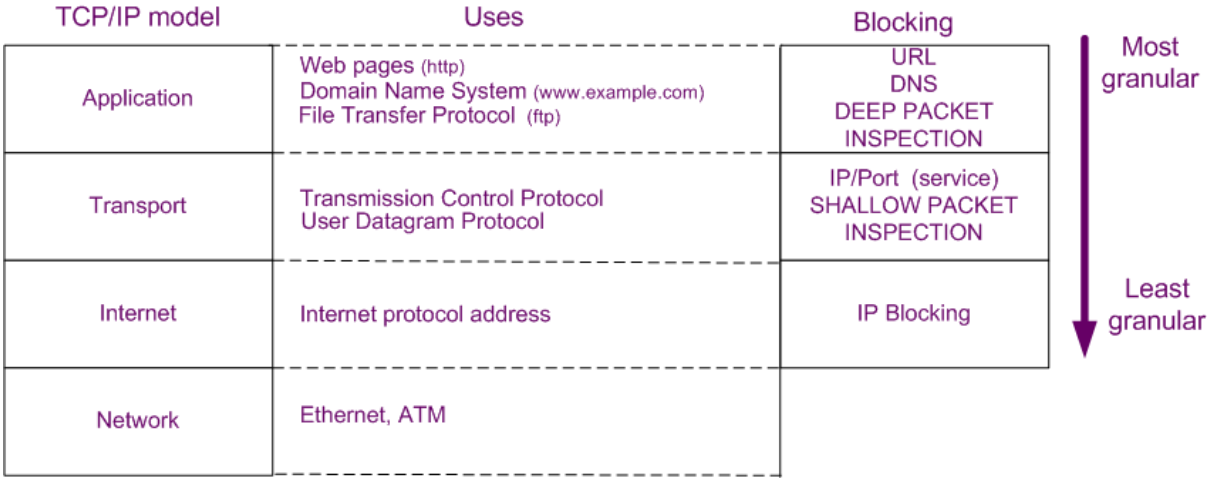
The TCP/IP protocol stack operates at four layers, each with its own functionality and interrelated purpose. The model is presented as a series of layers to help illustrate that there are discrete sets of tasks being undertaken. The lower the layer, the closer the set of tasks are to the operation of the physical network.

The Network layer is concerned with low-level transmission characteristics i.e. electronic signalling, hardware interface with the physical network medium such as, fibre optics or Ethernet. The Internet

layer is primarily concerned with the creation of data packets, routing and forwarding of packets to their destination according to the IP address contained in the header of the packet. The Transport layer defines connection requirements or reliability of data sent across the network. Finally, the Application layer defines interaction with lower Transport layer functionality and the external end-user program making the request, such as web browser or email client.

The blocking techniques we consider each operate at specific layers in the stack. The lower in the stack the blocking technique operates the less granular the blocking technique is.

Figure 4: Application of blocking techniques to the internet protocol suite



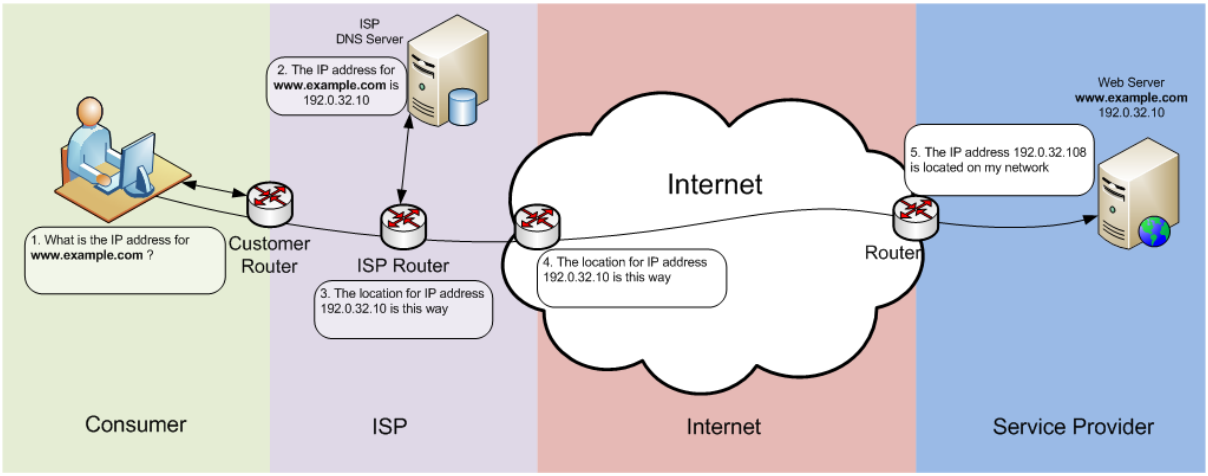
Source: Ofcom

It should be noted that the internet is not the same as the World Wide Web (WWW). The World Wide Web is comprised of web servers which serve up pages requested by web browsers. Within the web browser web pages are rendered, displaying text, images, animation and links to other web pages.

When a user requests and receives a web page – they are relying on a number of internet related services (see Figure 5), these include:

- Internet Service Provider connectivity (broadband);
- Domain Name System (translation of domain names into IP addresses);
- network routing; and
- Web server.

Figure 5: High-level overview of requesting a web page



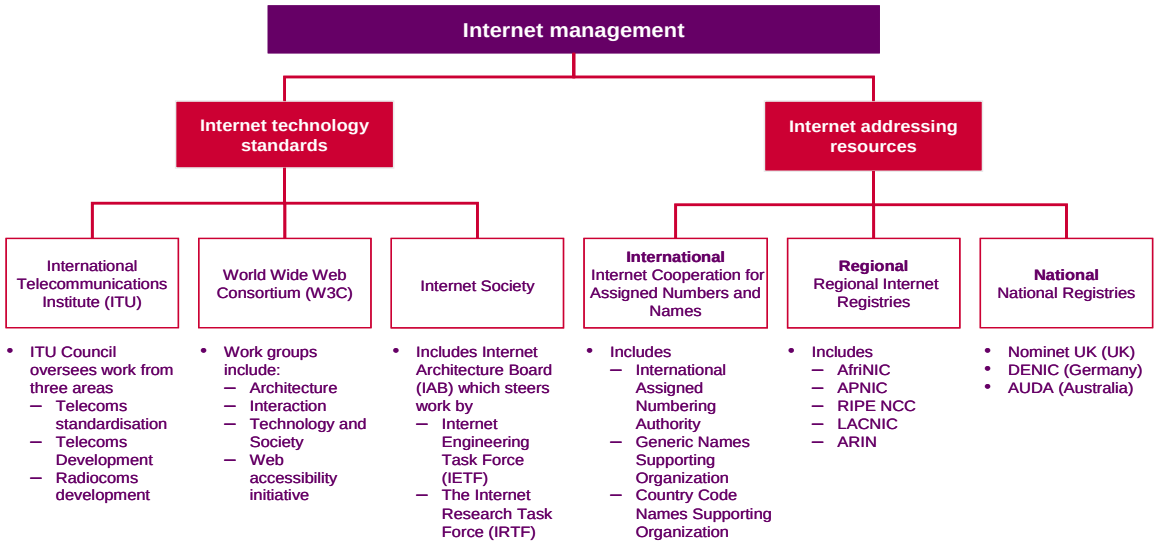
Source: Ofcom

3.2 Internet Governance

To understand some of the challenges to developing an effective site blocking framework it is important to have an appreciation of the systems of governance and administration which enable the smooth operation of the internet.

The administration and governance of the internet is a global undertaking involving national and international organisations (government and non-government). We do not attempt to explain here how the governance of the internet is structured in its entirety. Rather, we focus on the aspect of administration which is most relevant for this report, namely the system for registering details for the ownership of both Domain names and IP address blocks. There are challenges involved in reliably identifying the owners of individual sites which would make it difficult for a Court to identify and to contact the owner of a site should an application be received for a blocking injunction to be granted against that site.

Figure 6: Key internet governance bodies



Source: Ofcom

The Internet Corporation for Assigned Names and Numbers (ICANN) is a not-for-profit organisation, formed in 1998, which is responsible for a wide range of internet-related tasks which had previously

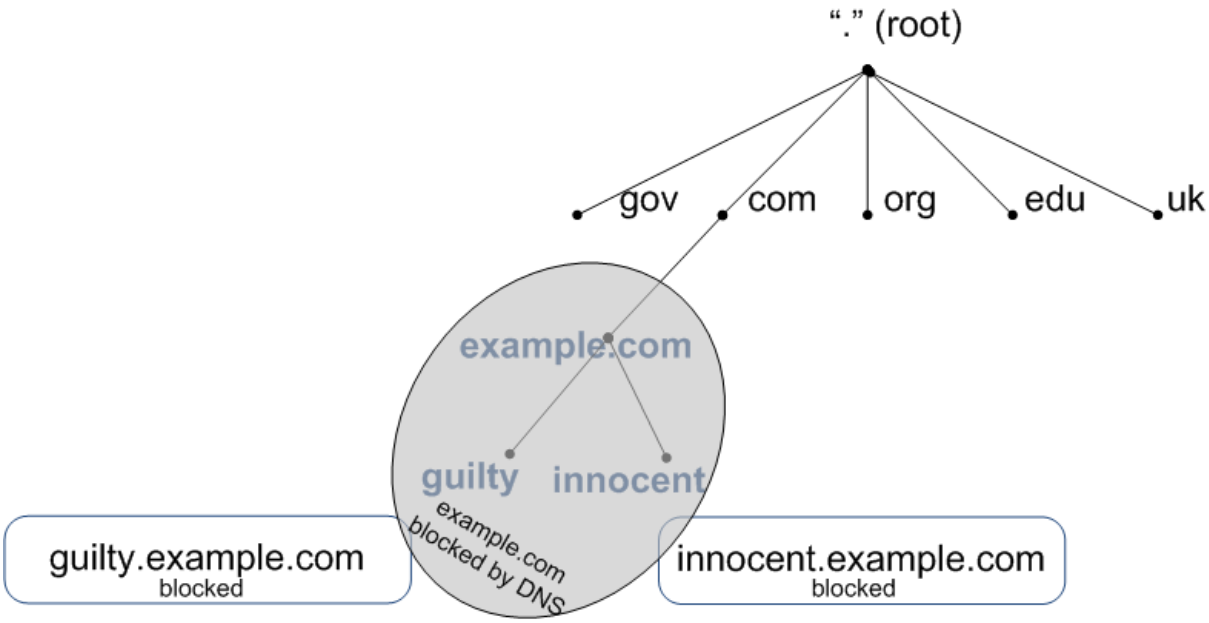
been undertaken by the US Government. Amongst them, it is responsible for coordinating and delegating the distribution and management of internet resources and DNS administration via the Internet Assigned Numbers Authority (IANA), the body established to oversee IP address allocation.

Domain Name System administration

ICANN delegates the administration of generic Top-Level Domains (i.e. non-country code specific domain suffixes such as .com, .net, .info etc) to third party organisations to oversee the domain registry activity. In turn the registry allows commercial companies to offer a Domain name registration service to individuals or organisations wishing to secure a domain name. These companies are known as registrars.

Country Code Top Level Domains (ccTLDs) such as ".uk" or ".fr" are administered by national independent registries operating on a country-by-country basis. Nominet is the UK registry responsible for managing the ".uk" domain suffix. Nominet is a not for profit organisation, funded by registration fees and is owned by its members.

Figure 7: Domain Name registration overview



Source: Ofcom

When an individual or company purchases a domain name from a registrar they are asked to complete domain contact details including their email and postal addresses. These details are then entered into DNS WHOIS. DNS WHOIS is a service provided by the DNS Registry that allows queries to the Domain Name database, such that the ownership of a particular domain can be established.

We understand there are no verification processes attached to registrant contact details (e.g. comparison to a credit card billing address). Moreover, Nominet allows private individuals to opt out of displaying full contact details if the site or service is used for non-commercial purposes (e.g. hobby sites). Where an individual has opted out in this way, a query of the registry database for ownership details returns only the name of the registrant.[18] To further complicate matters, some domain name registrants and registrars make use of privacy services which hold registrant details providing a generic contact somewhat analogous to an escrow or message relaying service.

Figure 8 below provides an example response to a WHOIS query against the Nominet registry for the Ofcom.org.uk domain.

[18] Nominet - WHOIS opt-out http://www.nominet.org.uk/registrars/systems/data/whoisoptout/

Figure 8: WHOIS – Ofcom.org.uk result (abbreviated)

Result of WHOIS query:

```
Domain name:
    ofcom.org.uk

Registrant:
    Ofcom (Office of Communications)

Registrant type:
    Unknown

Registrant's address:
    Ofcom (Office of Communications)
    2a Southwark Bridge Road
    London
    SE1 9HA
    United Kingdom

Registrar:
    NetNames Limited [Tag = NETNAMES]
    URL: http://www.netnames.co.uk
```

Source: Nominet

The accuracy of DNS registrant data, including contact details held by the various registries in the various WHOIS databases is reportedly highly unreliable. A 2010 study conducted on behalf of ICANN estimated that only 22% of WHOIS registration details within the sample set were wholly accurate and correct.[19] In only 46% of the sample was the data of sufficient quality for the researchers to be able to contact the registrants either directly or indirectly. Significantly, 28 % of the sample had major errors which led to a failure to contact the registrant. The remainder of the WHOIS data contained a range of different errors which could impede the ability of the Court (or any other party) to successfully contact the registrant.

Internet Resource Allocation

Where it is difficult to locate the owner of a domain through the DNS WHOIS database it may be possible to at least identify the hosting service provider through establishing which network operator has been allocated particular IP addresses. While domain names are allocated by DNS Registries, other internet resources, such as IP address blocks, are administered by five regional registries:

- AfriNIC - African
- APNIC – Asia and Pacific
- ARIN – North America
- LACNIC – Latin America
- RIPE NCC – Europe and Middle East

These five regional registries for internet resources also operate a searchable database for IP address and network routing information. Unhelpfully, this is also referred to in some cases as WHOIS. Whereas the DNS registries hold details about domain name owners, internet resource

[19] Draft Report for the Study of the Accuracy of WHOIS Registrant Contact Information

http://www.icann.org/en/compliance/reports/whois-accuracy-study-17jan10-en.pdf (17/01/2010)

registries provide contact details for the network owner/operator (e.g. which ISP or hosting company providing access and network services to a particular site).

The internet resource registry could serve as a contact point for bodies wishing either to make a complaint or to obtain further ownership or administrative information regarding the management of IP addresses. It can be used as a complement/alternative to the DNS WHOIS databases described above, but the database is not a complete record of IP address allocation and its value is dependent upon the accuracy of the information submitted by network owners. We understand that it is not mandatory for network operators to update contact details in the event of a change, creating a practical problem in reliably identifying the network which owns a particular IP address or range of addresses.

Figure 9: RIPE-NCC database (WHOIS) query Ofcom IP address (abbreviated)

```
% Information related to '194.33.160.0 - 194.33.179.255'
inetnum:         194.33.160.0 - 194.33.179.255
netname:         OFCOM-UK
descr:           OFCOM
country:         GB
admin-c:         TM3024-RIPE
tech-c:          TM3024-RIPE
mnt-by:          OFCOMUK-MNT
mnt-by:          RIPE-NCC-HM-PI-MNT
mnt-lower:       RIPE-NCC-HM-PI-MNT
mnt-routes:      OFCOMUK-MNT
mnt-routes:      COLT-CH-MNT
mnt-domains:     OFCOMUK-MNT
status:          ASSIGNED PI
source:          RIPE # Filtered
address:         Riverside House, 2a Southwark Bridge Rd. SE1 9HA
source:          RIPE # Filtered
```

Source: RIPE-NCC

Copyright owners have explained the difficulty they often have identifying and contacting site owners, largely for the reasons set out above, and how this has already hindered legal actions in the UK and in other countries. At best, these administrative weaknesses would slow down the process of identifying and contacting a site operator, but at worst it may be impossible for the Court to reliably identify and contact the site operator. This is particularly relevant where there is an incentive, as in the case of copyright infringement, to hinder of the process of identification of the site owner.

It should be possible to address this issue in practice. For instance, it could be made mandatory by Nominet (i.e. an element of Nominet's terms and conditions) for domain owners to provide verifiable contact details when registering a site and to ensure that those details remains correct where the ownership of a domain changes hands. Nominet would clearly have to check compliance regularly. The failure therefore to correctly register contact details could result in Nominet withdrawing the domain on the grounds that there had been a breach of the terms and conditions. This of course could only address a small subset of domains (i.e. those from .uk). International cooperation would be required to improve the administration of domain name registries more broadly.

It may be that the barriers to reliably identifying the owner of a particular site prove to be insurmountable, such that an alternative approach needs to be sought. The case study below briefly illustrates such an alternative. Subject to a court order, the US authorities are able to effectively take control of domain from the existing owner making the site and services inaccessible. These seizures are conducted with the co-operation from the US-based DNS registry. It is then for the affected site operator to come forward and challenge this action. Such an approach has merit where it is not possible to reliably identify a site operator. The credible threat of having access to a site blocked in such a way may also contribute to legitimate site operators ensuring that their contact details are correctly entered into the WHOIS database.

Case Study: ICE Domain Seizures

An approach to blocking access to allegedly infringing sites has been taken in the US which does not require that the site operator be contacted or given the opportunity to challenge the block prior to it being executed. The US Department for Homeland Security's Immigration and Customs Enforcement (ICE) division has, since 2010, taken ownership of the domains of a number of sites which are alleged to have infringed copyright law in the US. Under US civil forfeiture law, property can be seized pre-trial where there is a concern that it could be destroyed by the defendant before a trial has taken place.

ICE, under the authority of a Court order, switches the authoritative name servers for these seized domains and modifies the domain name records resulting in a redirection of network traffic. Visitors to the web sites are routed to a web server operated by ICE that displays a warning page. The domain seizures are executed with cooperation of the Registry controlling the generic top-level domain (gTLD). Where the sites are ".com" the company who has the ICANN contract for this gTLD is VeriSign (which also controls ".net" gTLD).

Most recently, in February 2011, ICE seized domain names of six services (operating via ten websites) allegedly video streaming premium sporting and pay-for-view events.[20]

- ATDHE.NET
- CHANNELSURFING.NET
- HQ-STREAMS.COM
- HQSTREAMS.NET
- FIRSTROW.NET
- ILEMI.COM
- IILEMI.COM
- IILEMII.COM
- ROJADIRECTA.ORG
- ROJADIRECTA.COM

Visiting nine of the ten sites via the web site produces the following warning page from the U.S. Federal authorities (*the other web site presented web pages containing generic advertising content*).

[20] New York investigators seize 10 websites that illegally streamed copyrighted sporting and pay-per-view events - http://www.ice.gov/news/releases/1102/110202newyork.htm

Figure 10: Federal holding page for seized domains

High profile enforcement action may serve as a deterrent to operators of infringing sites, in that having to find an alternative domain to operate under is an inconvenience. However, as an approach it has been shown to be susceptible to circumvention by the affected site operators. Of the six services targeted in February 2011, it is reported that five have since moved to alternative domains and continue to operate.[21]

This does not mean that all site operators would so readily seek to circumvent the measure, but it shows that where there is an incentive to do so then it is feasible. We are aware of circumvention measures reportedly available for end users, but we have no information on the extent of usage. For instance, a Firefox browser plug-in is reportedly available that allegedly automatically re-directs end users to those alternative domains, as well as to other sites seized by ICE.[22]

It is also reported that there has been significant over-blocking as a result of the ICE action. In one high profile case, it is claimed that access to 84,000 sites was blocked as a consequence of ICE seeking to block access to a single site.[23,24] It should be noted that were such an approach be implemented in the UK the scope of any seizures would be limited to ".uk" country code top-level domains.

[21] The sixth site was back in operation the following day, but was subsequently taken down by the operator following his arrest. See http://www.stormfront.org/forum/t795997/

[22] MafiaaFire Redirector :: Add-ons for Firefox: - https://addons.mozilla.org/en-US/firefox/addon/mafiaafire-redirector/

[23] ICE Confirms Inadvertent Web Site Seizures - InformationWeek:http://www.informationweek.com/news/security/vulnerabilities/229218959 (18/02/2011)

[24] News - http://freedns.afraid.org/news/ (12/02/2011)

With effective international cooperation amongst enforcement authorities the effectiveness of a seizure programme could be increased, but without such an approach it would be relatively trivial for a site operator to move to an alternative registry.

Section 4.

4. Blocking sites

4.1 Background

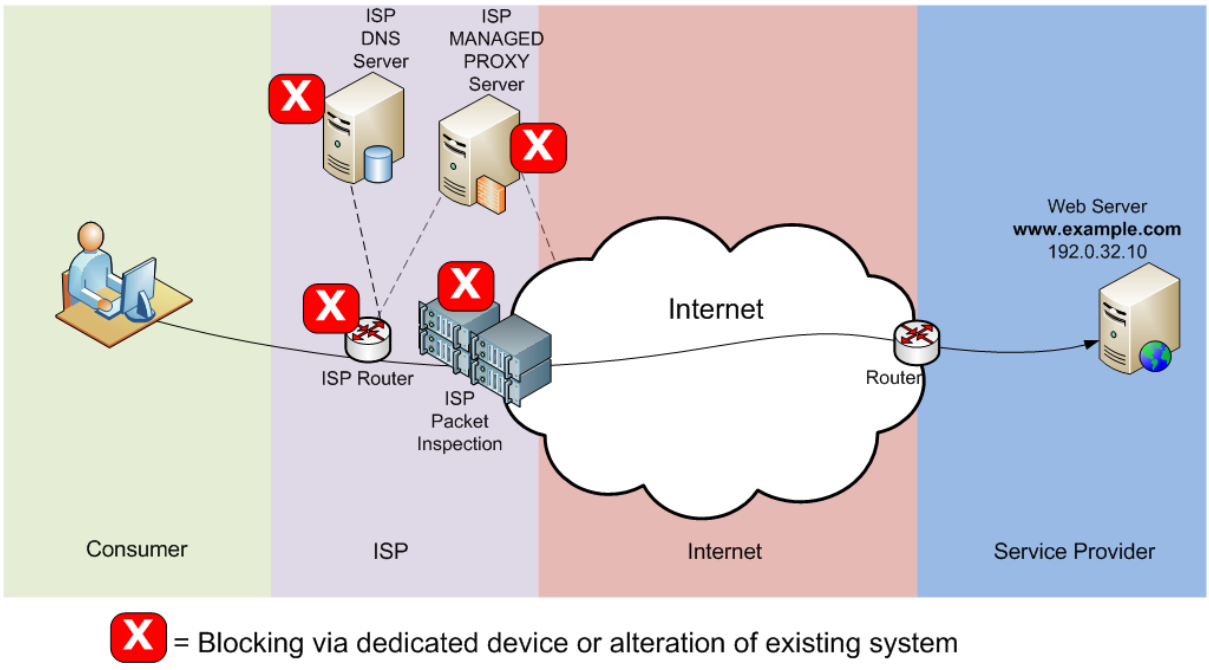
There are a number of technical methods which can be used to constrain access to sites on the internet. In this section we review the main techniques which are currently available to the main fixed line ISPs. We consider them in the context of the questions posed by the Secretary of State and, in particular, we highlight issues which we believe to be pertinent to any consideration of their deployment as part of a judicial framework.

When looking at existing site blocking techniques in use around the world we have decided to focus on currently used and known techniques:

- IP address (section 4.2)
- DNS (section 4.3)
- URL (section 4.4)
- Packet Inspection (section 4.5)

We refer to these as the primary techniques. Figure 11 illustrates possible deployment locations for each of the techniques.

Figure 11: Possible deployment locations for the different site blocking techniques



Source: Ofcom

We note that in discussions with stakeholders there were no further alternative approaches to site blocking proposed.

There are, in addition, tools available to ISP customers allowing for blocking to be implemented from within the home. For example software, analogous to anti-virus software, is available which allow users to specify specific sites to be blocked. It is feasible for router hardware manufacturers to offer additional functionality to both ISP and consumer router markets. This could include optional site blocking targeted at known infringing sites; such a capability would complement wider internet

parental control features. Some parents in particular may see value in having support from their ISP or router supplier where they wish to have greater control over how their accounts are used. Most recently, one ISP, TalkTalk, has launched a network level solution, offering users a range of controls over sites accessible by people using the account (see the case study below).

Although such in-home solutions are potentially of great value to users seeking a means of protecting themselves or their families from inadvertent infringement, we do not believe that these approaches are options for a judicial model. However, we would encourage the ISPs, software companies and router manufacturers to engage in discussions on what services they could credibly offer to consumers within this context.

Case study: TalkTalk HomeSafe

On the 9th May 2011, ISP TalkTalk launched for their customer base a free product, HomeSafe. Comprised of three elements HomeSafe is an ISP network based security and parental control package offered on an "opt-in" basis. When activated, the site blocking technology applies to all internet web traffic from the TalkTalk customer premises. HomeSafe is a joint venture between Symantec and Huawei.

TalkTalk customers can turn on or off features of HomeSafe via a password protected web portal (https://myaccount.talktalk.com). We understand once activated the web site blocking is operative within minutes.

HomeSafe offers a range of functionality:

Virus Alerts:

- Blocks access to websites that may harm computers i.e. infected with malware (viruses, Trojans). We understand it relies on a list of known malware distributing websites and an element of heuristic scanning.

Homework Time:

- Sets web browsing time restrictions, when operative blocks gaming and social networking web sites.

Kids Safe:

- Blocks access to categorised websites (dating, drugs, alcohol and tobacco, file sharing, gambling, pornography, social networking, suicide and self-harm and weapons and violence). TalkTalk customers are able to add further web addresses (URL) of other websites not included within the supplied categories.

Of particular relevance, TalkTalk offer customers the ability to block access to file sharing websites. TalkTalk define file sharing websites as "*websites that provide or promote file sharing applications*".

We understand the HomeSafe product utilises Deep Packet Inspection (DPI) technology which examines the contents of web requests against the known blocked site category lists that the TalkTalk customer has opted to block. TalkTalk customers and webmasters/site operators may request removal of the website from a blocking category if deemed inappropriate or incorrect.

In reviewing the techniques we consider the overall operational management overhead and the technical complexity of implementation of each technique for ISPs. All ISPs, in keeping with standard engineering practice, operate a change control process whereby routine non-emergency work is scheduled in advance. Some ISPs have stated that certain parts of their networks, such as core routing infrastructure and peering points, are highly critical and therefore changes are kept to an absolute minimum. The network change control window varies widely from ISP to ISP, from a few minutes to thirty days depending on the type, complexity and scale of proposed change. This may affect the ability of ISPs to implement certain site-blocking injunctions in a timely fashion and may make the selection of a highly automated site blocking technique more attractive.

This section also considers the ease with which site blocking can be circumvented, either by ISP customers or the blocked site operator. We then consider what countermeasures the ISP can take to reduce or halt such circumvention.

4.2 Blocking by IP Addresses

Background

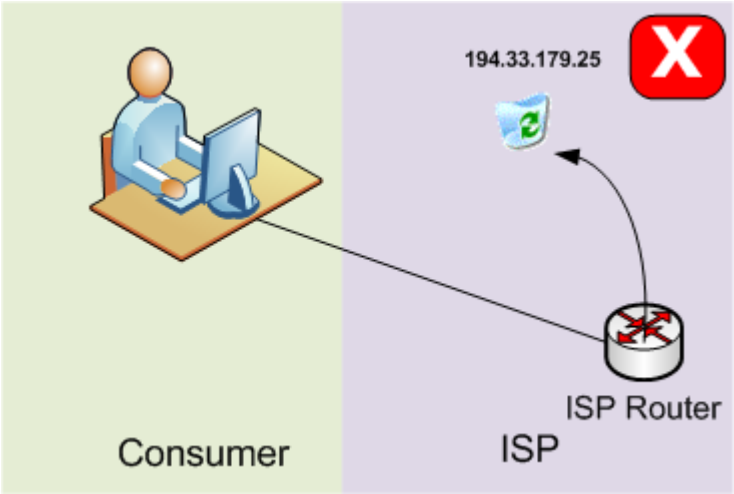
At the heart of the internet is a collection of networking technologies based on the Internet Protocol (IP), which is the standardised format for transmission of data across the internet. In the most widely used IP version, IP version 4 (IPv4), the address is comprised of four numbers separated by a dot ".", sometimes referred to as a "dotted quad" address. For example, the Ofcom web site has the public IP address of 194.33.179.25.

IP allows the sending of data to and from computers across the world in the form of packets. An IP packet contains the source and the destination IP addresses, as well as the payload or data. Each individual packet may take a different route to the destination address. The destination device is then able to reconstitute the original data based on the information contained in each packet, whether it is an e-mail message or a web page. The series of networks that make up the internet is connected via routers, which hold dynamic records of the nearness or best route for a given network (i.e. most efficient way for a packet to travel across the network) and forward each of the packets on to its destination.

Routers can be modified to send IP packets destined for a specified destination IP address to a non-existent or NULL route – effectively blocking access to the destination site. Similarly, an entire network range can be blocked by advertising the "best" route for a given network and likewise routing the packet to a NULL route.[25]

Figure 12 illustrates simply how IP blocking operates.

Figure 12: IP Blocking on routers



Source: Ofcom

Robustness

Bypassing IP address blocking is technically straightforward for those who have an incentive to do so.

The blocked site operator may:

- change IP address but stay on the same network (i.e. on the same hosting provider);

[25] Other network devices, such as traffic management/shaping equipment and Deep Packet Inspection devices, can also perform IP address blocking. However, the deployment of such devices is not universal amongst ISPs.

- move to an entirely new network (to a previously unobserved IP address);
- offer encrypted network services which obscure the true network address/destination such as Virtual Private Networking;[26,27] or
- server operators may institute a Fast Flux network (where users run software on behalf of blocked site which hides the true network address of the blocked site).

There are other methods available to site operators. When moving to a new IP address a site operator may register multiple IP addresses for a given site in order to maintain service in the event that some of those individual IP addresses are blocked. This approach has legitimate purposes also.[28] Furthermore, by setting a low "Time to Live" (TTL) Domain Name System (DNS) record value, determining the length of time that the IP address for a particular domain (expressed in seconds) remains in remote name server caches, it is easier for a site operator to move IP addresses without end users losing access. Where a low TTL is expressed the ISP DNS name server resolution cache is purged quickly thereby ensuring that newly assigned site IP addresses are retrieved from the authoritative name server and site accessibility is maintained. Figure 13 below shows that the TTL value for 'kickasstorrents' is one hour, demonstrating that any changes to IP address to DNS name are refreshed and propagated within ISP DNS servers in just over an hour.

Figure 13: Kickasstorrents DNS record Time to Live (1 hour)

Name	TTL	Class	Record	Address
www.kickasstorrents.com.	3600	IN	A	95.215.60.37
www.kickasstorrents.com.	3600	IN	A	93.114.40.112
www.kickasstorrents.com.	3600	IN	A	193.105.134.81
www.kickasstorrents.com.	3600	IN	A	95.143.195.138
www.kickasstorrents.com.	3600	IN	A	76.76.107.90

ISP customers may use anonymous web proxy (a server which acts as an intermediary between the end user and the site operator) or other anonymising services, such that the ISP is not aware that the end user is seeking access to the blocked site.

ISP technical response to customer bypass of site blocking

If circumvention techniques deployed do not use encryption then it is possible for the ISP to perform further scrutiny of the IP packet to aid the effectiveness of IP address blocking. An example could be to scrutinise all traffic destined for unencrypted web proxies and block any traffic which matched to a set of given rules or a particular packet signature. When a packet matching the blocked site IP address, destination host or even a particular keyword passes through a Deep Packet Inspection (DPI) device, which enables the reading of the contents of the packet as well as the source and destination IP address, the network connection can be terminated.

We explore blocking using DPI methods further in section 4.5.

[26] Ipredator - Surf anonymously with VPN and proxy https://www.ipredator.se/?lang=en

[27] UK based VPN services facilitating access to copyright infringed material may be subject to site blocking injunctions. UK VPN operators may institute site blocking at the VPN egress point. NB: we are not aware of any UK based VPN service marketed or positioned for such activity. Such services are likely to be non-UK based.

[28] To ensure high availability of services in the event of computing or network failure relating to a single IP address legitimate site operators will similarly use multiple IP addresses for sites.

Granularity of IP address blocking

IP address blocking does not offer a granular method of blocking internet sites. With the shortage of IP v4 addresses the need to ensure efficient use of those limited addresses and hosting business efficiency means that website hosting companies host multiple websites on shared equipment and resolving to a single IPv4 address. As a consequence there is a strong likelihood that the blocking of a single IP address would result in the blocking of access to multiple sites. Only the hosting provider will know how many sites share a particular IP address.

Estimates vary on the scale of IP address sharing between websites; a 2002 study estimated that 87% of websites shared an IP address within active COM, NET, and ORG web sites.[29] We are unable at this point to further verify and determine the current extent of sites sharing single IPv4 address. However, the sharing of IP addresses is common practice in the website hosting sector. Whilst some infringing sites are hosted on dedicated equipment or behind a single IP address this is not necessarily true in all circumstances.

IP address site blocking considerations

Some ISPs have expressed concern at the complexity of administering IP address blocking on routing equipment. These concerns included:

- router performance implications relating to the size and the growth of the blocked site IP address lists over time;
- the duration of the blocking injunction and the requirement to maintain these lists on routing equipment; and
- an inability to accurately predict costs as the number of sites likely to be blocked under Court injunctive process is not known to an accurate level at this stage.

Several ISPs stated that IP address blocking would require additional investment in network hardware and, dependent on volumes, increase operational overheads including staff numbers. These are, however, issues which can be addressed and, by themselves, would not be a significant barrier to using IP address blocking.

The deployment of IP blocking would also be under the aegis of scheduled system changes (change control), often-planned days or weeks in advance. Differing ISP change control regimes may lead to a site blocking order being executed and applied within different ISPs on different dates and times. Typically changes to networks that are designated routine are implemented faster than changes considered significant. The more risky a change (in terms of impact and potential issues to network services), the greater the level of technical impact analysis and due diligence required.

There is not in our view a consistent definition of the status (i.e. routine or major) of IP address blocking that is applicable to ISPs of all sizes. This may vary accordingly to the number of routing or network devices on which IP blocking is deployed. Some ISPs purchase internet access and bandwidth from wholesale higher tier providers. In these cases contractual agreements would be necessary to institute IP site blocking, particularly on 3rd party managed equipment. Whilst these operational issues would not seem to be insurmountable, they give an indication of the complexities involved in implementing a block.

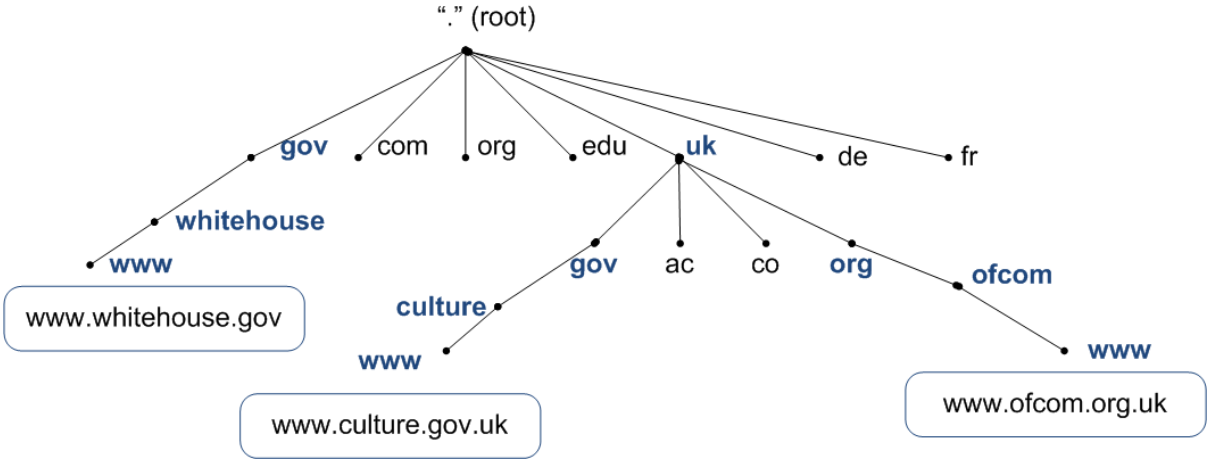
[29] Web Sites Sharing IP Addresses: Prevalence and Significance
http://cyber.law.harvard.edu/archived_content/people/edelman/ip-sharing/
Benjamin Edelman - Berkman Center for Internet & Society - Harvard Law School (September 2003). The study examined a subset of generic top level domains.

4.3 Blocking by DNS

Background

The current widely used version of IP, IP version 4, allows for approximately 4.3 billion unique IP addresses. To make the process of connecting to internet computers or hosts easier a hierarchal naming system was devised. Domain Name System (DNS) is a distributed database which allows the translation of human readable domain names into the all important IP address. The often used analogy to explain DNS is that it serves as the phone book for the internet. The process of finding the IP address for a given domain name via DNS is referred to as “name resolution”.

Figure 14: A partial view of the DNS hierarchy

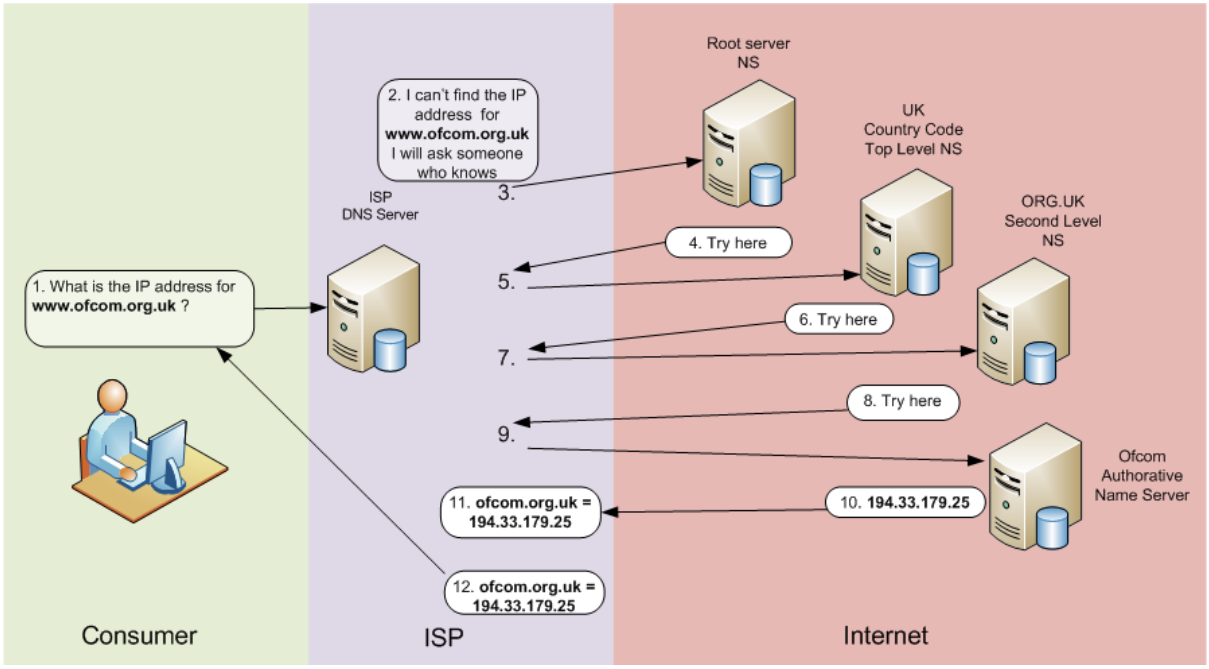


Source: Ofcom

When a fully qualified domain name, such as www.ofcom.org.uk, is entered into a web browser or other internet application the requesting computer sends the name query to the first name server configured in the broadband router or computer.

Typically if the first name server to respond cannot readily find the corresponding IP address within its memory or records then the name server will start at the root name server asking and receiving instructions to the query in a chain like sequence until either the IP address is found or not from the authorative name server. Figure 15 overleaf gives a high-level graphic overview of this process. If the IP address is retrieved from the name server tasked with holding the definitive record; the original requesting name server may insert the resultant record into memory (cache) and sends the IP address to the client.

Figure 15: Recursive name resolution process



Source: Ofcom

Blocking sites by DNS

The distributed nature of DNS and its key role in facilitating connection to internet hosts make it an obvious candidate to perform blocking of sites.[30] The ISP could institute a block via ISP DNS name servers by the following methods:

- hard coded entry to a designated IP address or to the special "localhost" address 127.0.0.1;
- modification of the DNS name server so that it refuses to undertake the query; or
- modification of the DNS name server so that query returns that the domain is non-existent (NXDOMAIN).

The manual alteration of DNS name server records may require a scheduled engineering time to perform the changes. We understand that manual alteration of DNS name server records generally require a restart of the DNS name server process in order for the change to come into effect. During the restart of a DNS server end-users will be unable to perform name resolution queries against the restarting service, this activity may require careful scheduling by the ISPs as to avoid interruption to end-user services. We do not consider this to be a major barrier to deployment as it is a process which would typically take less than one minute to complete.

Some vendors of name server software provide an automated DNS blocking solution that does not require restarting of services when new domains are added to the blocking list. These DNS based systems are primarily targeted against malicious domains containing malware or used in Phishing websites. Such a solution could be adapted to meet the needs of site blocking under section 17 of the DEA.[31]

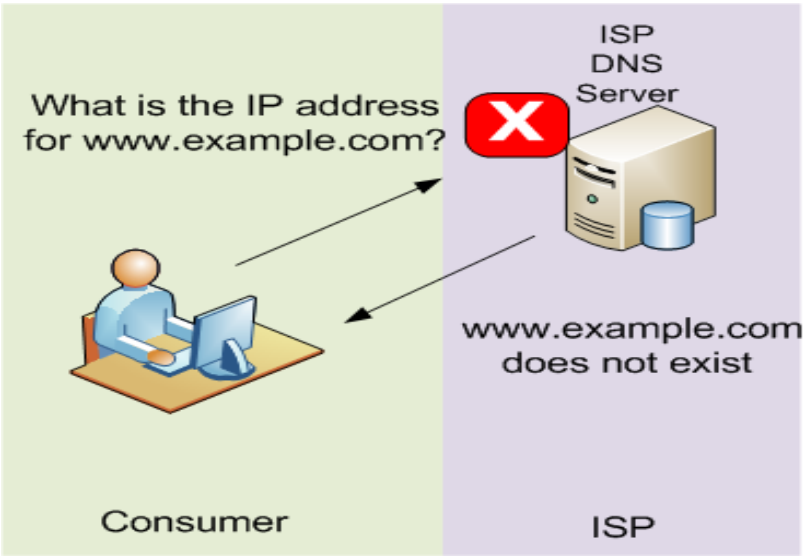
[30] The Italian Amministrazione autonoma dei monopoli di Stato - AAMS (Independent Administration of State Monopolies) compiles lists of gambling domain names which Italian Internet Service Providers block via manipulation of DNS name server queries.

[31] Vantio MDR™ | Malicious Domain Redirection Software | Web Redirection - Nominum.com

http://www.nominum.com/what-we-do/software-systems/vantio-mdr

Figure 16 illustrates how DNS blocking works in practice.

Figure 16: DNS blocking



Source: Ofcom

DNS blocking robustness

For site operators and end users with a sufficient incentive to engage in circumvention DNS blocking is technically relatively straightforward to bypass:

- the blocked site may offer services such as Virtual Private Networking, which is where encryption and other security measures are deployed to ensure that the data cannot be viewed by third parties (DNS name resolution may occur within the VPN providers network thereby bypassing the ISP based DNS site-blocking);
- the end-user can change their DNS name servers to 3rd party DNS name servers;[32,33]
- users may use anonymous web proxy or other anonymising services which are not reliant on the ISP DNS servers; or
- name resolution may be performed locally by adding an entry to a hosts file (IP address resolution information can be obtained from websites running a web-enabled equivalent of "nslookup" command).

For end users who want to bypass blocks there are several options. For instance, there are many legitimate alternative DNS providers to ISP DNS registries. Examples include OpenDNS and Google DNS. We consider the changing of DNS servers to alternative providers to require low technical skills, as the providers offer clear instructions using plain English. For instance, switching to Google DNS requires 11 steps for Windows users and only 8 for those using MAC OS.

With a modest understanding of internet technologies it is possible to access a site by entering the site IP address (if multiple websites are hosted at the same IP address the user will be displayed the default web site or page for that web server/IP address). Site operators can draw attention to online

[32] Google Public DNS - http://code.google.com/speed/public-dns/

[33] OpenDNS Store > Sign up for OpenDNS Basic: - https://store.opendns.com/get/basic/

web based and alternative sources of DNS name resolution within emails to their user base or via online forums.

Other channels that site operators could use to widely distribute advice on how best to circumvent DNS blocking could include posting to online forums, Really Simple Syndication (RSS) or updates via micro blogging sites such as Twitter ®. The advice could include changing to unblocked DNS name servers, Virtual Private Networks and proxy services or other anonymising systems.

Similarly, site operators may quickly mirror or make copies of a blocked site on new top level or country code domains pointing towards new IP addresses e.g. www.blockedsite.cc; www.blockedsite.ru; www.blockedsite.vn; www.blockedsite.net.

ISP Response to blocking circumvention

Internet service providers could employ further countermeasures to prevent name resolution requests being transmitted to other DNS providers. This may require the discarding of DNS name resolution traffic to non-ISP based name servers. This technique requires further scrutiny of IP packets, described in more detail in the document section “Packet Inspection”.

One potentially unwelcome side effect of blocking non-ISP DNS traffic is that providers of legitimate 3rd party DNS services (some of which filter responses based on category e.g. adult, gambling for parental controls or business filtering) or businesses that run their own DNS services may also be blocked using this approach.

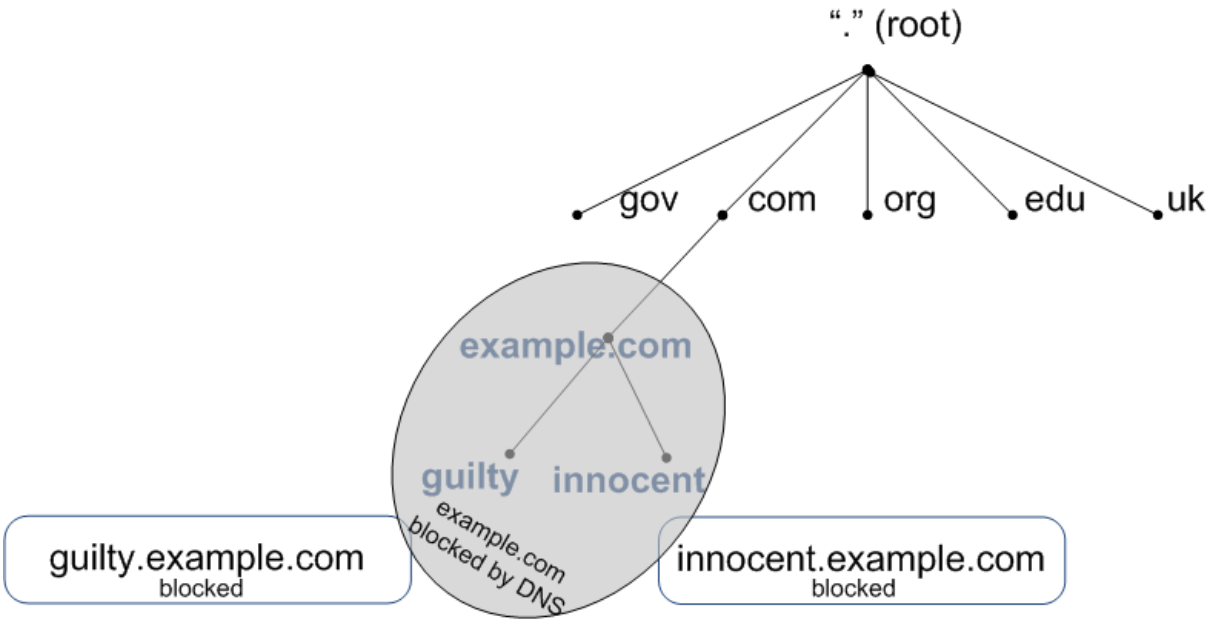
Where an ISP customer uses an ISP supplied broadband router it is technically feasible to “lock down” the router DNS name server IP address settings to prevent querying non-blocked DNS name servers. We understand this may require a change to the ISP terms and conditions and would preclude the use of 3rd party DNS providers, some of which offer family friendly or malware domain blocking services. We do not know how many service providers or end users would be affected by such a measure. The extent of subscriber own-supplied broadband routers connected to the ISP networks is unknown and limiting or locking down a non-ISP broadband router configuration is not, in our view, realistically feasible.

Granularity of DNS blocking

We understand DNS blocking is executed against the uppermost level of the infringing domain, which means that all services operating within that domain zone are also blocked. This would not be a concern where all of the services within the domain zone were infringing, but care would be needed where lawful services were being served from within the same zone as infringing services. This is illustrated below, where a block instituted against the domain “example.com” blocks both “guilty.example.com”, which was the target site and “innocent.example.com” which was not the intended subject of the block.

This is not an insurmountable problem. It may be that the Court could consider the relative amounts of infringing and lawful content within the relevant domain and reach a view on whether the amount of infringing content within the domain zone was sufficient to justify blocking access to all sites within the zone. Such an approach, perhaps complemented by some form of notice and take-down, may create an incentive on legitimate domain owners to take greater care over the nature of the content available on the domain.

Figure 17: Illustration of DNS over blocking risk



A web server is capable of serving web pages either from the familiar sub domain "www.example.com" or uppermost level within their zone, "example.com". This means that DNS blocking may not always be technically reliable. For instance, a study of blocking in the German North-Rhine-Westphalia state revealed that 44% of ISPs failed to block correctly a Neo Nazi website using DNS blocking. [34] However, effective monitoring of the operation of a block should be sufficient to minimise the risk such an outcome.

DNS site blocking considerations

We believe the costs incurred by implementing DNS blocking would be incremental. Some DNS software vendors already offer customers an add-on to DNS systems that blocks malicious domains. Our current understanding of the ISP DNS name server infrastructure leads us to believe that site blocking is possible using the manual insertion of blocked Domain Name records or by the use of an automated system and so could be implemented in a timely manner.

4.4 URL site Blocking

Background

Perhaps the most familiar use of the Uniform Resource Locator (URL) is the World Wide Web (WWW). A URL can point to a specific file, directory or server.

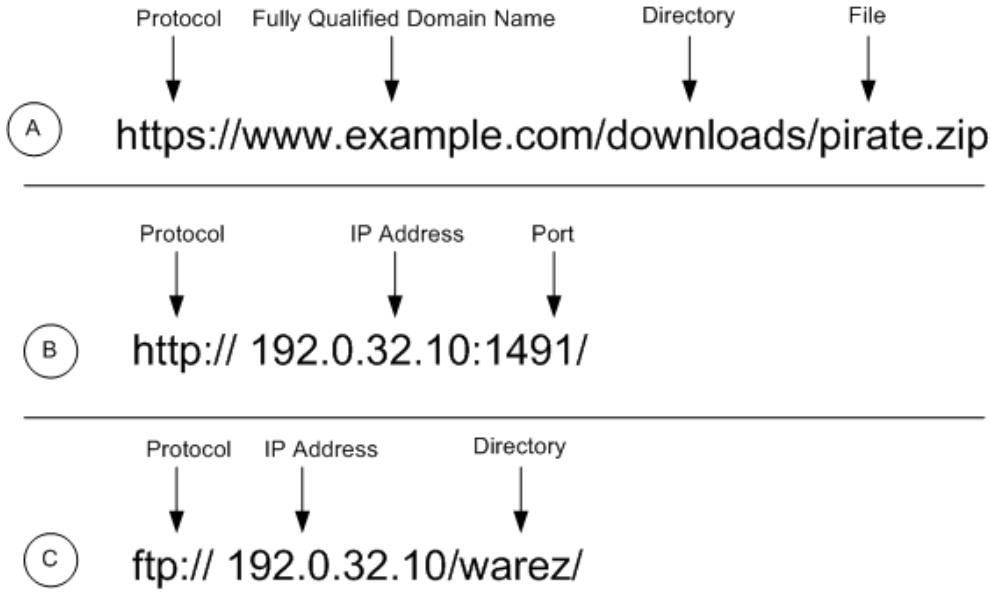
Figure 18 below shows a web URL secured by HTTPS, web URL of web server running on a non-standard network port (1491) and a File Transfer Protocol (FTP) URL accessed via the host IP address. There are other services that make use of the URL format including News Groups and legacy internet technologies[35].

[34] The Electronic Library of Mathematics - Maximillian Dornseif - Government mandated blocking of foreign Web content

http://subs.emis.de/LNI/Proceedings/Proceedings44/GI-Proceedings.44.innen-42.pdf

[35] RFC 1738 - http://www.ietf.org/rfc/rfc1738.txt

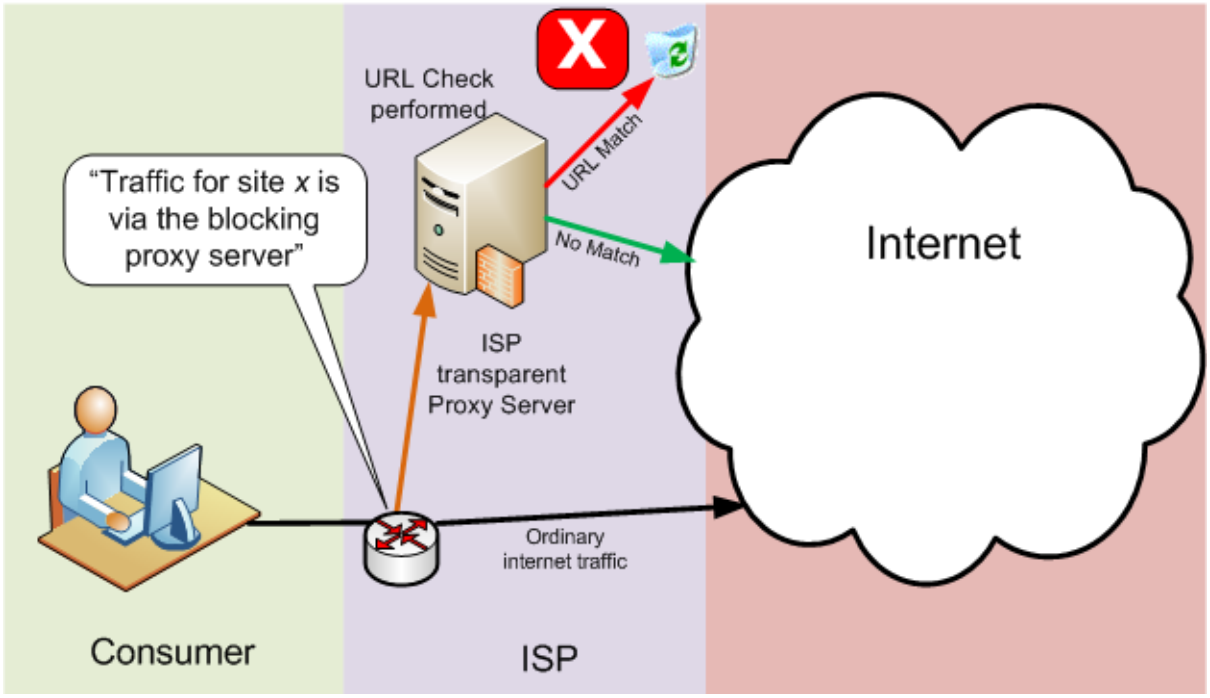
Figure 18: Example URLs



Source: Ofcom

Figure 19 provides an illustration of URL blocking:

Figure 19: Model URL transparent proxy blocking



Source: Ofcom

A proxy server is an intermediary server that handles connection requests on behalf of the requestor. Proxy servers are common in schools and businesses, performing a number of functions including the caching of content, blocking of inappropriate sites and providing some rudimentary security. Before the advent of broadband internet content caching proxy servers were commonplace in early dial-up ISP infrastructure and deployed inline (all traffic would usually pass through the proxy server).

Most UK ISPs are currently operating a URL blocking scheme, constraining access to abusive images of children. This scheme is overseen by the Internet Watch Foundation (IWF) and the explained briefly in the case study below.

Case study: the Internet Watch Foundation and URL blocking

The UK Internet Watch Foundation (IWF) is a charitable self regulatory body founded in 1996. [36] Today the IWF membership includes ISPs, mobile operators, web filtering software vendors and search providers. At the heart of the IWF operation is activity to combat access to online child sexual abuse material.

One of the key IWF tasks is the distribution to ISPs and mobile operators, both in the UK and internationally, of a list of web URLs that contain child abuse images. The IWF operates a hotline for members of the public to report online child abuse material.

Once a reported URL is verified the IWF will add it to the existing URL list. The blocking URL list is distributed from the IWF and incorporated into blocking systems at the ISPs.

Details of the blocking technology used by ISPs are confidential in nature. The description below gives a general overview of a "model" deployment. The model blocking technology is implemented as a transparent proxy reliant on the alteration of network route metrics. There are some communications providers that display a web page detailing why the block has taken place. However, this approach is not universal.

An outline of a "model" IWF URL blocking process is as follows:

the URL to block is http://www.example.com/download/pirate.zip :

- The URL is added to the blocking proxy server.
- The "best" network route to the offending site is advertised by ISP network equipment as via the blocking proxy server. All traffic destined for www.example.com is rerouted to allow for the exact URL matching to take place.
- The request on reaching the proxy server undergoes a detailed comparison.
- If a direct match is found the connection is halted (either directed to warning page or dropped).
- If the request does not match the blocked URL traffic it is allowed to continue.

URL blocking robustness

Blocking via URL can be instituted either at the domain level (e.g. www.example.com) or to a specific URL (e.g. http://www.example.com/files/pirate.zip). Arguably, if applied at domain level URL blocking retains the same over blocking characteristics as DNS based blocking (some copyright holders have expressed a preference during meetings with Ofcom to require the blocking of whole domains/sites rather than discrete URLs).

URL blocking is limited in its value as it can only block web traffic. It is not suited to addressing infringing content found on Newsgroups of transferred via file transfer protocol (FTP), a standard protocol used to transfer files from one host device to another. Its limited scope has been cited as one reason why a group of Dutch ISPs are reported to have backed away from introducing an IWF-style blocking list in the Netherlands.[37] There is an obvious concern that the use of URL blocking could simply see the shifting of infringing content to Newsgroups and FTP technologies, meaning that any benefits derived from blocking were short lived.

Techniques that may undermine URL blocking include:

[36] Self-regulation | Internet Watch Foundation (IWF) - http://www.iwf.org.uk/members/self-regulation

[37] https://www.bof.nl/2011/03/07/dutch-providers-abandon-ineffective-web-blocking/

- web site operators providing encrypted access to their web sites via Secure Sockets Layer/ Transport Layer Security i.e. https connectivity https://www.example.com/downloads/pirate.zip;
- a site operator may run a website on a network port other than port 80;
- the site operator changing the IP address and bypassing the network routing announcements;
- a site operator registering a new domain name e.g. www.example.net or www.example.org;
- the blocked site offering services such as Virtual Private Networking;
- the use of anonymous web proxy or other anonymising services;
- the site operator reorganising the site structure if the blocking is conducted against specific URLs; and
- the site operator or end user encoding URLs to bypass blocking.

ISP Response to blocking circumvention

There are other dedicated network devices which can be used to the same effect of dropping IP/Port combinations of traffic. These include firewalls and DPI devices. Such blocking techniques are technically easily bypassed using VPNs, Anonymous Proxies, and other anonymising tools.

Granularity of blocking URLs

Although it is reported as being expensive to implement effectively, URL blocking can be highly granular against web URLs, with low levels of over-blocking when applied at the level of the URL. In general URL blocking is effective only against unencrypted web traffic. We understand that the blocking of other unencrypted traffic containing URLs, such as News Groups and FTP, is theoretically possible, but we are not aware of any commercially available solution which does so.

Proxy based blocking can be applied at the domain level e.g. www.example.com or to a discrete URL level e.g. http://www.example.com/downloads/pirate.zip.

URL site blocking considerations

As previously described, the method by which a typical blocking transparent proxy is deployed may require the rerouting of traffic to the proxy network segment. A blocking injunction on a popular site with heavy traffic may slow the performance of both the proxy server and the network segment where the proxy server is located. Even if a match is rarely made for a particular site all traffic must pass through the blocking proxy, causing congestion.

Several ISPs have commented that any deployment of URL or domain based blocking should not dual use the IWF system. The rationale is twofold; firstly, there is the concern that a blocking proxy server or other systems deployed for copyright infringement purposes would likely be targeted for hacking or malicious activity.[38] Compromise of dual use system puts at risk the activity related to the IWF. Secondly, should the blocking proxy fail due to loading issues this may put at risk IWF blocking. However, it may be that there are opportunities for the sharing of some facilities and systems, and therefore costs, such that the integrity of the IWF system would not be undermined. But we do recognise the risks involved.

One ISP expressed concern around the increased levels of inserted network routing announcements directing blocked traffic to a URL blocking proxy server, as described in the “model” IWF implementation. An example cited by an ISP was the risk of accidentally recreating the widespread

[38] The Sidney Morning Herald - Australia cyber attacks could last 'months' http://news.smh.com.au/breaking-news-technology/australia-cyber-attacks-could-last-months-hackers-20100211-nuzc.html

rerouting to a “black hole” as exemplified by 2008 Pakistan Telecom network reroute of YouTube traffic. This activity severely impaired access to YouTube for around two hours. [39]

Dedicated URL blocking systems that do not alter the source characteristics of the traffic are emerging. Reportedly, the New Zealand Government is using devices that are a hybrid of router and URL blocking technology[40] for IWF type activity. Such devices may yield blocking performance increases over Proxy based URL blocking. We understand that deployment of multiple devices within the ISP network is possible, however further technical analysis and performance modelling is required. Similarly, in view of the concerns expressed about the risk to the IWF model, further examination of the concerns raised by ISPs would be sensible before any decision was taken to implement URL blocking.

4.5 Blocking by Packet Inspection

Background

Packet inspection involves the contents of the packet being examined in transit, rather than simply the IP address of the source and destination devices. Network packet inspection can be applied at two levels: ‘shallow’ and ‘deep’.

Shallow packet inspection could reasonably be described as blocking based on the IP address, port and protocol combination e.g. all traffic destined for IP address 192.0.32.10, TCP on port 80 (web traffic) is dropped. It is possible using this approach to maintain access to other services, such as e-mail or FTP, at the blocked site.[41]

Deep packet inspection devices examine the content of a network packet for characteristics or values. DPI technology is commonly used within Intrusion Prevention and Detection Systems that protect systems from malicious activity. The DPI device may rely on signatures, anomaly detection or examination of traffic flows. IP packets may become fragmented when passing through network topologies with differing properties. In these circumstances the DPI device will reassemble the packets in order to perform analysis.

If the DPI device encounters a network packet or packets that match certain pre-defined properties e.g. traffic destined for a blocked site, the DPI device can inject a reset command, thus breaking the connection or simply drop further traffic destined for the blocked site. Careful consideration of the blocking or matching criteria employed by the DPI equipment is required. A failure to do so may lead to the blocking of legitimate traffic (false positives) or the passage of infringing traffic (false negatives).

Blocking unencrypted traffic is technically trivial. Blocking encrypted traffic is more problematic. Blocking on an IP address/network protocol/port combination shares similar over-blocking characteristics for web servers sharing a single IP address (we believe this over-blocking characteristic applies even if the virtual web servers are running SSL/TLS encrypted sites distinguished by SSL/TLS Server Name Indication).[42,43]

---

[39] YouTube Hijacking: A RIPE NCC RIS case study — RIPE Network Coordination Centre: - http://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study

[40] New Zealand relies on BGP router protocol to filter the 'Net - http://arstechnica.com/tech-policy/news/2010/03/new-zealand-relies-on-bgp-router-protocol-to-filter-the-net.ars

[41] This may present opportunity for the site operator to reconfigure services in a non-standard way thereby defeating the shallow packet inspection, however there are end-user usability considerations with the operation of services in a non-standard way.

[42] Transport Layer Security (TLS) Extensions http://www.ietf.org/rfc/rfc4366.txt

[43] NameBasedSSLVHostsWithSNI - Httpd Wiki - http://wiki.apache.org/httpd/NameBasedSSLVHostsWithSNI

It is possible to block outbound encrypted traffic connection requests to a known, specific IP address, by the use of router Access Control Lists (ACLs). An ACL is a rule that can block or drop traffic for a given IP address if using a particular port (e.g. port 443). ACLs use additional routing and network equipment computational resources, as it requires comparison of each IP packet against the ACL rule base. Careful performance and capacity planning is required to avoid a decrease in network performance. Some router vendors have introduced software enhancements to improve the processing of ACLs, but this approach is by no means universal. Some models of routing equipment have set capacity limits for the number of ACLs that can be implemented.

An alternative approach to router ACLs is the deployment of packet filtering firewalls and traffic management devices. Firewalls are usually deployed at the perimeter of a private network facing an un-trusted network such as the public internet. It is feasible to deploy firewalls at various locations within an ISP network configured to discard or send reset packets when traffic is encountered meeting blocking rule base i.e. IP address and network port of the blocked site.[44]

Network performance is a consideration for the deployment of DPI devices. In order to maintain network throughput the ISP may have to divide network traffic into smaller capacity links and deploy multiple DPI devices capable of operating at high speed to reduce the network performance impact.

Packet inspection blocking robustness

Both shallow and deep packet inspection can be bypassed by site operators using the following means:

- changing the IP address but staying on the same network;
- moving to an entirely new network (to a previously unobserved IP address);
- the site may use network encryption techniques such as Virtual Private Networking to render scrutiny of the IP packet's payload or real IP address destination impossible, given the technology available today; or
- the site operator may add or remove site IP addresses from a pool of IP addresses.

End users who wish to circumvent packet inspection may opt to use anonymous web proxies or other anonymising services.

ISP response to blocking circumvention

Arguably, no single technical countermeasure exists to prevent bypass of packet inspection based blocking techniques. In the event that circumvention did occur, an alternative approach could be that copyright owners seek blocking injunctions against sites offering facilitation or bypass services such as VPN services and anonymous proxies. This would require that the Court be convinced that these services were facilitating access to infringing material, or were being used for the purposes of infringing. Alternatively, copyright owners could engage with providers of VPN services over a form of notice and take down, where VPN providers who did not take steps to effectively address infringement on their service could be subject to a blocking action in the UK. Legitimate users of VPN services would therefore know which services were at risk of being blocked when choosing their VPN supplier. Blocking of access to VPN services would clearly represent a significant escalation and would require careful consideration.

Packet Inspection site blocking considerations

Of the techniques considered, DPI is the only one to combine a highly granular approach with being able to catch all forms of unencrypted traffic. Some ISPs already deploy packet inspection systems in their network for traffic management and other purposes, so we assume that it can be deployed, albeit that this would involve a high level of complexity and cost for those not already running such

[44] Ignoring the Great Firewall of China - Clayton et al - University of Cambridge - http://www.cl.cam.ac.uk/~rnc1/ignoring.pdf

services. It may be that in the short to medium term DPI could only be deployed by the larger ISPs given the capital investment required.

Considerable care must be taken when using DPI devices to ensure compliance with relevant data protection, privacy and interception rules. The potentially intrusive nature of the technology means it would be feasible for service providers to have access to personal data, some of which may be sensitive. Clearly, measures to safeguard the legitimate interests of users would need to be adopted to complement any use of DPI.

4.6 Hybrid blocking

In some circumstances a combination of site blocking techniques may theoretically be more robust against circumvention than techniques used in isolation, although it is important to recognise that this is not always the case. Several end user bypass techniques are effective for a single or hybrid blocking (i.e. where a combination of primary techniques is used) approach, for instance VPN, anonymising tools**.** In addition, we have found no reliable evidential sources that demonstrate the use of multiple site blocking techniques is more effective against circumvention than the use of single techniques**.**

We believe that IP address based site blocking is not granular and is likely to lead to over-blocking. This may undermine the confidence in any site-blocking scheme, and create significant liability risks for service providers. The over blocking property is a by-product of sites sharing IP addresses. It is also worth noting the relative ease by which site operators can move to a new IP addresses. Moving to a new IP address is unobserved and transparent to the end-user who typically relies on a domain name to connect to internet services such as web sites. We have therefore discounted the use of basic IP address blocking as either a primary or secondary blocking technique.

We consider the use of a hybrid blocking of techniques using DNS based blocking as the primary means, reflecting our view that DNS blocking is the most suitable of the primary techniques for site blocking at the current time.

DNS blocking could be implemented alongside SPI. The SPI in these circumstances could be deployed to prevent the use of 3rd party DNS name servers thereby adding an additional obstacle to circumvention.

Alternatively, DNS blocking could be deployed alongside URL based blocking. In this deployment scenario, URL based blocking traps unencrypted web requests to blocked sites even if the end-user is using a 3rd party DNS server.

Finally, DPI could be deployed to supplement the effectiveness of DNS blocking. In this scenario, DPI is configured to intercept and block any unencrypted network traffic destined infringing sites; this traffic may have made use of alternative sources of DNS name resolution.

As with the deployment of any of the single primary techniques, the hybrid approach is also susceptible to circumvention by the use of anonymising tools such as The Onion Router, VPNs or anonymous proxy services.

4.7 Technological developments impacting site blocking

Background

The longer-term viability of some current techniques for blocking access to locations on the internet is open to question. In this section we briefly examine known emergent internet technologies which we consider may have a significant impact on how a site blocking scheme might operate. Given the rapid pace of technological change in this area, and the sorts of issues summarised below, any legislation to provide for a site blocking scheme would need to allow for a broad range of potential developments rather than being tied to the technologies which exist at the current time.

DNSSEC

The UK, along with many other countries, has started the deployment of DNS Security Extensions (DNSSEC). Digital signatures verify the source authenticity of DNS name queries, in a "chain of trust". DNSSEC is a key technical response to DNS cache poisoning, a technique exploited by cybercriminals to re-direct end users of a web site to another site of the hacker's choosing. This may lead to the user innocently providing sensitive data to the hacker or downloading malware from the site.

DNS blocking, which relies on the modification of DNS records from a non-authoritative source, is arguably a blocking technique that undermines the benefits of DNSSEC. A DNSSEC aware client expects a digitally signed response to a name request. The digital assurance extends to a name server reporting that a domain is non-existent.

Should client functionality emerge, such as an operating system or browser alert that indicates the questionable authenticity of the authority status of a blocked name query, it may lead to an undermining of the confidence in DNSSEC and potentially cause confusion.

DNS RPZ

Berkley Internet Naming Domain (BIND) is widely deployed open source DNS server software. The software is freely available and incorporated into many UNIX and Linux based operating systems. BIND is supported and developed by the Internet Systems Consortium. Version 9.8 of BIND fully incorporates Response Policy Zones (RPZ)[45]. DNS RPZ allows DNS name servers to receive updates from a centralised server data relating to internet domains which are blacklisted. Conceptually similar to email SPAM blacklists, DNS RPZ was originally devised to address the issue of phishing and malware websites. DNS RPZ could conceivably be deployed for anti-piracy site blocking activity. We understand that, as yet, there are no known live production deployments within North American ISP market or direct support from alternative name server software vendors.

IPv6

As of the 12th February 2011[46] IPv4 addresses are now considered exhausted, and the next generation of Internet Protocol addresses is being gradually adopted by network providers, vendors and businesses. IPv6 offers a near inexhaustible supply of unique IP addresses (2^{128} unique available addresses). It is inevitable that consumers and site operator will adopt IPv6 addressing. There is an emerging trend of tunnelling IPv6 traffic within IPv4 traffic, which we believe also significantly reduces the effectiveness of site blocking. IPv6 devices in future will be able to change IP address configuration and network location more rapidly[47] than the current widespread IPv4 allows. The implications of IPv6 in relation to site blocking are not, at this stage, fully understood.

Cloud technology

We believe private Cloud based services such as storage will play a part in future copyright infringing and blocking techniques. For example, an infringing website could utilise Cloud based storage. The storage layer is accessible from the web server or access layer using Virtual Private Networking connectivity. The website or service could move from IP address to IP address, geographic territory and jurisdiction, change DNS name and reorganise its structure whilst leaving the underlying storage layer intact. We believe this model could be particularly useful to cyberlockers.

Similarly Cloud based computing resources could be deployed in URL matching or transparent proxy blocking. With sufficient bandwidth, an ISP could divert traffic for a given website via a Cloud based proxy. As computing demands increase, the system acquires computing resources to match.

---

[45] DNS Response Policy Zones (DNS RPZ) (December 2010) - http://ftp.isc.org/isc/dnsrpz/isc-tn-2010-1.txt

[46] FAQ: IPv4 Exhaustion — RIPE Network Coordination Centre - http://www.ripe.net/internet-coordination/ipv4-exhaustion/faq

[47] RFC 2462 - IPv6 Stateless Address Autoconfiguration - http://www.faqs.org/rfcs/rfc2462.html

At this point we do not believe that Deep Packet Inspection (DPI) technology is suited to Cloud like deployments. The act of reassembling and matching IP packets without creating network bottlenecks is an inherent limitation of DPI technology. A more shallow approach is the scrutiny of destination IP address and network port. This approach is currently used for traffic management e.g. the shaping of P2P and Newsgroup network traffic at peak times.

Other technologies which could potentially play a role are currently in development. For instance, some ISPs have already deployed Packet Inspection and traffic management technology for the purposes of traffic shaping. It has been suggested that perhaps Packet Inspection offers a potential alternative high throughput blocking capability in the future, but data protection and privacy concerns are likely to constrain development of such invasive techniques. However, it is reasonable to assume that technical innovation will continue and ever more sophisticated blocking and filtering techniques will develop.

4.8 Conclusion on blocking techniques

It is our current belief that the blocking of discrete URLs, or web addresses, is not practical or desirable as a primary approach. Infringing website operators can readily change the structure of a websites, particularly commonplace database driven websites. We therefore recommend that if site blocking is adopted it should be implemented at a domain level.

We believe that in the short-term site blocking by DNS based blocking is currently the quickest to implement. DNS blocking impedes the resolution of a domain name to an IP address. We note that many ISP DNS servers are able to implement blocking via software vendor supported functionality or via the manual insertion of blocking DNS records. In the longer term however, the widespread adoption of DNS Security Extensions (DNSSEC) will be incompatible with DNS based blocking. The incompatibility rests with alteration, via the ISP blocking DNS server, of an ordinarily digitally signed DNS query responses to both successful name resolution responses and non-existent domain resolution responses. We would therefore anticipate that a replacement for DNS blocking would be required within the next three years.

Introducing a secondary blocking measure alongside DNS blocking may help further to deter the casual bypass of site blocking. Such measures, as previously outlined, could include URL blocking based on the widely understood transparent proxy blocking (UK IWF) or emergent hybrid routing technology as reportedly deployed in New Zealand.

In the medium to longer term we consider that deep packet inspection techniques are likely to provide a more robust approach to blocking than DNS. Although costly to implement today, we would expect that costs will fall as the larger ISPs invest in DPI devices for other purposes. However, for it to be part of a legislative approach the cost burden for smaller ISPs would need careful evaluation as would legal concerns related to compatibility with privacy, data protection and interception rules.

A summary of our review of the techniques against the core criteria for assessment is presented in the tables below.

Table 3: Summary of reviewed blocking techniques

Assessment criteria

Blocking technique	Speed of implementation	Cost	Blocking effectiveness	Difficulty of circumvention	Ease of administrative or judicial process	Integrity of network performance	Impact on legitimate services / law abiding consumers
IP address	Implemented on existing routers	Low cost	Poor – not granular	Easy by site operator & various ways by end-user	Difficult to determine accurately true IP address	Overhead on routing equipment – limits to number of blocking IP addresses	Over-blocking - sharing of single IP address by many sites
DNS	Modification of existing service	Marginal incremental cost	Prevents the resolution of IP addresses. Infringing sites services relying on domain resolution will be unavailable	Easy. Use of 3rd party UK or overseas DNS, new domain registration, end-user bypass, mirroring to new domains.	Identification of infringing domain	None known on general performance – DNSSEC adoption will impact	Multi-user websites, sub-domains, where whole domain is blocked.
Shallow Packet Inspection	Implemented on existing routers	Low cost if implemented only on routers – costly on firewalls devices	Poor – not granular	Easy by site operator & various ways by end-user e.g. encryption, anonymity networks	Difficult to determine accurately true IP address of infringing site	Overhead on routing equipment – effect on network speeds	Over-blocking sharing of single IP address by many sites
Deep Packet Inspection	Lengthy planning and deployment of new equipment within ISP network	Costly – long term matching of traffic volume network demands against DPI	Able to inspect and interrupt infringing traffic to web, newsgroups, FTP and other non-encrypted traffic	Evade by use of encryption, anonymity networks	Definition of blocking trigger e.g. domain name , GET request or key phrase within a network packet.	Considerable impact. Multiple devices and possible redesign of some network elements. Network performance as packet assembly required. Long term implications of IPv6 not fully understood	Potential for false positives /false negatives. Privacy and interception concerns
URL	Planning and deployment lengthy	Costly – hardware, software	Moderate effective only against unencrypted web traffic.	Site operator can reorganise site with ease, thereby creating new URLs. Evade by use of encryption, anonymity networks	Complex to implement against URLs – speed of URLs change; Easiest to target domains within injunction process	Using the BT IWF Clean Model requires rerouting of traffic for examination. Potential for network bottlenecks	Highly targeted in URL mode. Shares the same over-blocking characteristics when blocking against domains.

Table 4: Summary of potential hybrid blocking techniques

	Assessment criteria						
Blocking technique	Speed of implementation	Cost	Blocking effectiveness	Difficulty of circumvention	Ease of administrative or judicial process	Integrity of network performance	Impact on legitimate services / law abiding consumers
Hybrid: DNS & DPI	Planning and deployment lengthy.	Cost profile likely to exceed DPI blocking alone	Effective only against unencrypted network traffic. Can inspect and block many types of network traffic e.g. Web, FTP, NEWS	Evasion by use of encryption, anonymity networks	Use of blocking against domains and even traffic types possible	DPI element places demands on network infrastructure	Shares some characteristics with DNS blocking
Hybrid: DNS & URL	Planning and deployment lengthy.	Costly – hardware, software for URL blocking.	URL blocking acts on requests by users attempting to bypass via 3rd party DNS servers. URL blocking effective only against unencrypted web traffic.	Evasion via encryption, anonymity networks – new domain registration, mirroring	Accurate identification of infringing domain required	Effect of URL network bottlenecks reduced as DNS acts as first line defence.	Blocking of multi-user websites remain a risk. The impact of DNSSEC remains.
Hybrid: DNS & SPI	Shorter development and planning anticipated – interoperation would testing	Cost profile not dissimilar to DNS if using existing routers – dedicated equipment will increase cost	SPI acts to either block off network 3rd party DNS or infringing site	Evasion via encryption, anonymity networks – new domain registration, mirroring on new domain/site	Accurate identification of infringing domain required	Potential for performance issues when using SPI on routers –	If SPI is implemented against off network 3rd party DNS may harm legitimate businesses. Other aspects of over-blocking remain.

Section 5

5. Effectiveness of Section 17 & 18

5.1 Introduction

A key question the Secretary of State has asked us to consider is how effective sections 17 and 18 of the DEA are in providing for an appropriate method of generating lists of sites to be blocked.

For measures intended to address online copyright infringement to have the best chance of changing the behaviours of site operators and end users the risk of being caught engaged in infringing activities and of enforcement action being taken must be credible. The more effective the framework can be at fairly processing and issuing a large number of applications the more credible will be site blocking as an enforcement measure. Ultimately, the framework can only be effective in generating lists of sites to be blocked if copyright owners choose to make use of it at sufficient scale.

The purpose of this section is to set out the key characteristics for a site blocking scheme such that it would be used at sufficient scale to make enforcement action a credible threat. We then consider the challenges faced by the Government and by the Courts in implementing such a scheme.

5.2 Existing site blocking powers vs. the Digital Economy Act 2010

Copyright owners in the UK already have two routes to securing blocking injunctions against allegedly infringing sites on the internet.

Firstly, in an action for breach of copyright, a Court could issue an injunction requiring the allegedly infringing party to refrain from a particular wrongful act, including the infringement of copyright, and therefore to stop making infringing material available on a website.

In addition, section 97A Copyright Designs and Patents Act (CDPA) enables the Court to grant an injunction against a service provider where they have *actual knowledge* that their service is being used by another person to infringe copyright. Copyright owners have informed us that they have made only two applications to secure a blocking injunction. In the first case, where an application was made by Twentieth Century Fox (and others) to block access to Newzbin, the judge refused to grant the injunction for several reasons, including:

- the injunction can only be granted in relation to the material in respect of which rights are owned by the applicant. The injunction sought would have covered both works in which copyright was owned by the applicants (or persons on whose behalf they were authorised to act) and copyright in respect of works which they themselves did not own; and

- that while Newzbin would have known about some of the infringements taking place on its service it could not possibly have known about all the infringing activities for which the injunction was being sought.

The second case, where the Motion Picture Association has applied for an injunction requiring BT to block access to Newzbin2, a successor site to Newzbin, will be heard in July 2011 (the application for the injunction was made in December 2010).

Copyright owners have offered a number of arguments for why they have been reticent to make use of the blocking provisions in section 97A. They are concerned at the narrow scope of any injunction (i.e. that it covers only the specific content which was the subject of the application) and that there is no general obligation placed on the service provider to take measures to tackle infringement as a result.

As the injunction can be granted only when there has already been an infringement it would appear to be unsuitable for securing injunctions to prevent a future infringement. This makes section 97A less suited to cases where the concern is the streaming of live events or where the copyright material is valuable pre-release content or software.

They have said that there is a lack of clarity on what standard of evidence is required for a determination that a service provider has actual knowledge of the specific activity that the application is seeking to address. They also have concerns about the time taken to get a hearing once an application has been made. The application for a blocking injunction against Newzbin2 was made in December 2010 and a hearing is scheduled for July 2011. Copyright owners have told us that the cost of supporting a process such as this is a barrier to the smaller copyright owners taking action and makes sense only where the site in question is responsible for a significant amount of infringement. Some copyright owners also expressed a concern that an unfavourable outcome (from their perspective) could establish an unhelpful precedent which could send a signal that the barriers to successfully obtaining an injunction were too high for it to even provide a credible threat when copyright owners engaged with site operators on an informal basis to secure the taking down of infringing content.

The DEA introduces a framework for website blocking injunctions, the detail of which is to be provided by regulations made by the Secretary of State. The relevant provisions, set out in sections 17 and 18 of the Act, allow for a framework for injunctions which is potentially much broader than that which operates under section 97A. For instance, under section 97A, a service provider must have actual knowledge of another person using their service to infringe copyright. Under the DEA, the knowledge of a service provider or lack thereof is not a relevant consideration. Rather, the determining factor is whether the location (i.e. site) *"has been, is being or is likely to be used for or in connection with an activity that infringes copyright"*.

Moreover, an injunction under the DEA provisions may be granted on the grounds that a site is likely to be used for an infringing purpose in the future or to facilitate access to an infringing site at some time in the future whereas section 97A allows an injunction to be granted only where an infringement has already taken place. However, under both section 97A and section 17 of the DEA, copyright owners or their representatives would still need to demonstrate that the alleged infringement related to copyright in works owned by them (or by persons who had authorised them to act). This may not be a simple process as the Newzbin case demonstrates.

Copyright owners have explained that, under the right conditions, they would be seeking to take action against a number of sites totalling the low hundreds. In order to do so they have said that they would expect the judicial process to lead to injunctions being in place within a very short time period (potentially within hours) of an application being made. This reflects the concern that some copyright owners have about the rapid loss of value from live events being streamed on infringing sites and from the need to prevent access to pre-release movies and music before they become too widely shared for enforcement action against infringing sites to be effective or even credible. Given the speed at which site operators can implement circumvention techniques a lengthy gap between an application being made and a block being implemented undermines the effectiveness of the blocking scheme.

However, it is not clear that injunctions under section 17 of the DEA might offer the solution sought by copyright owners in terms of speed and flexibility. As regards the speed of granting an injunction, the first hurdle for copyright owners will be to notify service providers and site owners. As set out above, section 17(6) provides that a Court may not grant an injunction unless notice of the application has been given to the site owner and this may prove difficult for a copyright owner to ascertain. Whilst section 17(7)(b) permits any regulations to provide for notice to be given by publication in the case of site owners, we anticipate that a certain period from publication would need to be allowed to enable site owners to ascertain whether an application had been made in respect of their site and this would therefore introduce a period of delay prior to any hearing.

Even where the identity of the site owner may be determined, any hearing of an application is unlikely to occur within the short timeframe sought by the copyright owners since a site owner must be given the opportunity to present evidence to the Court in order for the Court to take account of such evidence as required by section 17(5)(a). The copyright owner must also provide evidence of what steps they have taken to ensure that the content in question has been made available through lawful means and this is likely to further prolong the process. The Court must also consider whether the injunction would be likely to disproportionately affect the legitimate interests of any person or would undermine freedom of expression. In addition, as set out above, copyright owners would still need to demonstrate that they owned the copyright in relevant works on the site (or were authorised to act on the owners behalf) and this will further complicate any consideration of the evidence.

Furthermore, copyright owners appear to want any injunction to be broad in scope to enable a flexible approach to circumvention by site operators. However, an injunction may only be granted in respect of individual "locations" (i.e. sites) rather than more generally sites operated by the alleged infringer. Therefore, it may be possible for circumvention to occur by re-establishing the site at a different location relatively quickly following the grant of an injunction and a copyright owner would need to apply for an injunction preventing access to that new location.

5.3 Ensuring that the legitimate interests of site operators and end users are protected

There is a particular pressure for any process leading to an injunction in this area to be fair. Where there is a perception that the process is unfair it would be reasonable to assume that there would be an increase in incentives to circumvent any block imposed rather than invest in the engagement with the legal process. To that end, the measures included in the DEA to protect the legitimate interests of site operators, service providers and end users should be noted.

The DEA provides that the Court may not grant an injunction unless the service provider and the relevant site operator have been given notice of the application. This would appear to be intended to ensure that those parties are given the opportunity to engage with the legal process and make representation to the Court should they choose to do so. This would be particularly important where the proposed block would impact on the legitimate interests not only of the site operator or service provider, but where the legitimate interests of end users and other parties would be adversely impacted. Such engagement would also help the Court to determine whether the service in question was providing access to a substantial amount of infringing content. However, as discussed earlier, the lack of a reliable method for identifying the owner of a site may prove challenging to any Court which is seeking to issue an injunction in a timely manner. Copyright owners have explained to us that their inability in many cases to identify and contact a site operator has hindered efforts to have content taken down or access to sites blocked in a number of countries.

The risk of over blocking, which may be relevant whichever technique was used to block access to a site, would place additional burdens on the process. Where there was a potential risk to the legitimate interests of other site operators, for example those sharing the same IP address as the targeted site or operating within the same domain zone, then it may be the Court would have to consider what impact a block would have on those parties, as well as the end users of those sites. It is unclear from the DEA how such issues would be treated in practice.

ISPs and user groups argue that any appeals scheme should be available at no charge to end users or site operators. They argue that any charge for appeals could reduce incentives for even legitimate services to challenge injunctions through the proper processes, rather than adopting circumvention measures. This would require sufficient transparency that site operators and end users actually had knowledge that a site had been blocked by order of a Court on copyright infringement grounds. Interested parties would also need to be provided with sufficient information on how to appeal or apply for a lifting of the blocking injunction. If it appeared difficult then there is a risk that affected parties would simply choose to circumvent the block, rather than follow due legal process.

A further complication arises from a consideration of the terms of any injunction. If the injunction is drafted in very narrow terms, preventing access to a specific IP address, for example, it will be very easy to circumvent and will require copyright owners to return to the Court for injunctions regularly in respect of the same infringing site since the IP address can be easily changed at very short notice. As a result, the measures would be likely to be ineffective at preventing access to sites offering infringing content.

Alternatively, an injunction may block access to the location of the site on which infringements are allegedly taking place by allowing service providers greater flexibility in the measures taken to block access to such sites. However, if the terms of the injunction are not sufficiently precise, service providers will be placed in a difficult position. On the one hand, they will need to ensure that they are in compliance with the terms of the injunction in preventing access to a particular site. On the other hand, if they go beyond the terms of the injunction, there is a risk of exposure to commercial liability where this results in over blocking which also covers legitimate sites. The terms of the injunction will therefore need to be precise as to the techniques which service providers are required to employ and the manner in which they are to be employed in order to provide certainty for service providers as to what they need to do. The balance between flexibility to respond circumvention and certainty for the

service provider may not be an easy exercise for a Court to commit to the terms of an injunction in the majority of cases.

5.4 Effectiveness of sections 17 and 18

On the basis of the above analysis, any injunction scheme operated under sections 17 and 18 of the DEA is unlikely to give rise to a sufficient level of actions to have a material impact on levels of copyright infringement. Copyright owners' expectations for a speedy process, with blocks implemented potentially within hours of an application being made, do not appear realistic given the constraints imposed on the Courts by the DEA, the need for a process which is fair to the legitimate interests of site operators and end users, and the practical challenges arising from the current state of site blocking technologies and internet governance.

If the Government was minded to pursue the objective of implementing a site blocking scheme, we would recommend that further research be undertaken to identify and evaluate alternative legal frameworks which would be more suitable. In particular, we would suggest any research considers how to best harness the potential value of complementary approaches, such as search engine de-listing, measures to constrain advertising and subscription revenue sources, as well as notice and take down approaches. Site blocking could potentially be more effective if it was supported by the appropriate use of such measures.

Section 6.

6. Conclusion

The Secretary of State for Culture, Media and Sport asked that Ofcom undertake a review of certain aspects of how sections 17 and 18 of the Digital Economy Act 2010 might function. Specifically, we were asked to consider whether there were techniques which the major fixed line ISPs could employ in order constrain access to prohibited locations on the internet, how granular they could be, the ease by which they could be circumvented and whether there were anti-circumvention measures available to ISPs. We were also asked to consider whether section 17 and 18 could enable the introduction of a process which would be effective at generating lists of sites for service providers to block.

We considered four techniques which are currently available for deployment. We reviewed each of them individually and considered also three possible hybrid options, where three of the four techniques could be deployed in combination. The techniques we reviewed are:

- IP address
- DNS
- URL
- Packet Inspection

In conclusion, we believe that it is certainly feasible to impede access to prohibited sites using any of the techniques we considered. ISPs in the UK have, for some years, operated a blocking scheme to impede access to child abuse images on the internet (through the Internet Watch Foundation) and blocking happens also in other countries for a variety of purposes, for example, to constrain access on political or religious grounds. Spain is an example of another European country which has passed legislation which, when finally implemented, would see the introduction of a blocking scheme.[48]

We identify, however, a number of concerns regarding each technique which the Government should be aware of should the Secretary of State move to give effect to sections 17 and 18.

Of the techniques we consider to be most effective, only blocking based on Deep Packet Inspection would appear to offer a level of granularity where over blocking would not be a major concern.[49] The use of DPI is not, however, without risk, as it raises privacy issues, and is extremely complicated to implement, based on current technologies. DNS blocking would perhaps offer a simpler and less expensive option, but it is likely to be fully effective only until DNSSEC is implemented, so is perhaps not a long term solution. IP address blocking is simply not granular enough and the ease by which is can be circumvented would suggest that it is not a suitable technique candidate. URL blocking is currently used, but its limited scope and ease of circumvention would suggest it has at best a complementary role to play alongside DNS blocking.

However, we find that sections 17 and 18 are unlikely to be able to provide for a framework for site blocking which would be effective. We do not believe that it is possible to deliver a framework under the DEA which simultaneously meets the requirements of the copyright owners for a timely implementation of blocks and a flexible approach from service providers to tackling circumvention, with the need to respect the legitimate interests of site operators, service providers and end users.

However, site blocking could still play an important role in helping to tackle online copyright infringement. Further research would be required to identify the most suitable policy framework for implementing such a scheme.

---

[48] We understand that the Spanish Government is currently preparing the secondary legislation necessary for implementation.

[49] URL blocking is also highly granular, but its limited scope means we do not consider it to be an effective blocking technique for tackling online copyright infringement.

Site blocking could be made more effective where it is supported by complementary measures, such as search engine de-listing and notice and take down processes. Such measures would help to address the known limitations of the techniques we review. For instance, a notice and take down process may reduce the potential harm from over blocking by providing an opportunity for site operators to remove infringing content and so ensure the continued availability of legitimate content which may otherwise have been inadvertently blocked. Search engine de-listing would make it harder for operators of blocked sites to re-establish their service, such that users could easily locate it.

Consideration could also be given to ensure the cooperation of VPN providers to secure the blocking of infringing sites. VPN providers would be asked to assist with blocking infringing sites accessed by their customers. Those that do not take part with such a scheme could, in turn, find their own service at risk from blocking provisions. Such a scheme would constitute a significant further escalation, and would therefore require very careful analysis and consideration

Circumvention of a block is technically a relatively trivial matter irrespective of which of the techniques used. Knowledge of how site operators and end users can work around blocks is widely distributed and easily accessible on the internet. It is not technically challenging and does not require a particularly high level of skill or expertise.

There is limited research on end-user behaviour in this area. One small scale study estimates that circumvention levels, albeit in a different context, may be as low as 3% of end-users, despite there being a high level of understanding of circumvention measures.[50] Although beyond the scope of our study, we believe it may be possible to position a site blocking scheme in such a way as to minimise incentives to circumvent. For instance, if the process for granting injunctions is perceived to be fair to the legitimate interests of site operators and end users then there will be less reason to seek to circumvent the block.

More broadly, if the site blocking scheme was to be positioned as part of a wider mix of measures, such as education, and supported by the effective development and promotion of attractively priced and convenient lawful services then the incentives of consumers to continue to use infringing services could be reduced. As a result levels of circumvention would also be lower than might otherwise be expected. We believe that further research is needed on the mix of complementary measures which might create an environment where there is a change in social culture and levels of tolerance of online copyright infringement.

We note that, under the DEA, Ofcom has a responsibility to report on an annual basis to the Secretary of State on a range of matters, including education initiatives, measures taken by copyright owners to make their content more accessible online and the degree to which targeted civil actions have taken place against egregious infringers. We believe that this research might provide a useful vehicle for assessing the potential effectiveness of different mixes of measures, but any report would not occur until twelve months after the start of the notification scheme under the Initial Obligations Code. We would be happy to work with Government and other stakeholders on ways to allow this research to happen sooner.

[50] 2010 Circumvention Tool Usage Report, Berkman Centre for Internet and Society, http://cyber.law.harvard.edu/publications/2010/Circumvention_Tool_Usage

Annex 1

Technical Glossary

Access Control List (ACL)	Network technology that can allow or disallow traffic to destinations or services
Anonymous Web Proxy	Service that allows users to place web requests via an intermediary server. The proxy server makes the connection on behalf of the user thereby hiding originating IP address and bypassing blocking network techniques.
Authorative DNS name server	DNS name server that answers authoratively for a given zone
Domain Name System (DNS)	Global hierarchal distributed database. Allows translation of domain names e.g. www.example.com -> 192.0.32.10
Hypertext Transfer Protocol (HTTP)	Application protocol used usually between web servers and web browsers
Hypertext Transfer Protocol Secure (HTTPS)	Encrypted HTTP using Secure Sockets Layer/Transport Layer Security. Data between web browser and web server is encrypted. Data transmitted is private. HTTPS prevents eavesdropping or alteration of data. Used widely for online credit card purchases. Web browser padlock symbol denotes HTTPS secure connection.
Internet Protocol (IP)	Packet based network protocol.
Network Port	Designated connection number allows multiple services to operate on the same host and standardised connectivity.
Peer-to-Peer (P2P)	Network technology used for the efficient distribution of content. Widely used for unauthorised distribution of copyright content.
Recursive DNS name server	Server that performs translation of domain name on behalf of the user. Typically caches responses to improve performance for subsequent requests.
The Onion Router (ToR)	Anonymity network originally developed by the United States Navy. Used in many countries to bypass state censorship.
Transmission Control Protocol (TCP)	Connection orientated reliable network protocol.
Uniform Resource Locator (URL)	Method of requesting and locating resources on web servers, File Transfer

User Datagram Protocol (UDP)	Connectionless unreliable network protocol
Virtual Private Network (VPN)	Technology that facilitates secure private data communications over the internet via encrypted network connections. Used for a variety of purposes including remote access for business workers.

Annex 2

WHOIS domain privacy service output

Federally seized domain (02/02/11)

```
Whois v1.01 - Domain information lookup utility

Sysinternals - www.sysinternals.com

Copyright (C) 2005 Mark Russinovich


Connecting to COM.whois-servers.net...

Connecting to whois.PublicDomainRegistry.com...


InvisionArg S.A


Domain Name: ILEMI.COM


Registrant:


    PrivacyProtect.org

    Domain Admin        (contact@privacyprotect.org)

    ID#10760, PO Box 16

    Note - All Postal Mails Rejected, visit Privacyprotect.org

    Nobby Beach

    null,QLD 4218

    AU

    Tel. +45.36946676


Creation Date: 29-Sep-2009


Expiration Date: 29-Sep-2013

Domain servers in listed order:


    ns90.ilemi.com

    ns91.ilemi.com

    ns92.ilemi.com
```

ns93.ilemi.com

Administrative Contact:

PrivacyProtect.org
Domain Admin (contact@privacyprotect.org)
ID#10760, PO Box 16
Note - All Postal Mails Rejected, visit Privacyprotect.org
Nobby Beach
null,QLD 4218
AU
Tel. +45.36946676

Technical Contact:

PrivacyProtect.org
Domain Admin (contact@privacyprotect.org)
ID#10760, PO Box 16
Note - All Postal Mails Rejected, visit Privacyprotect.org
Nobby Beach
null,QLD 4218
AU
Tel. +45.36946676

Billing Contact:

PrivacyProtect.org
Domain Admin (contact@privacyprotect.org)
ID#10760, PO Box 16
Note - All Postal Mails Rejected, visit Privacyprotect.org
Nobby Beach
null,QLD 4218

AU

Tel. +45.36946676

Status:ACTIVE

PRIVACYPROTECT.ORG is providing privacy protection services to this domain name to protect the owner from spam and phishing attacks. PrivacyProtect.org is not

responsible for any of the activities associated with this domain name. If you wish

to report any abuse concerning the usage of this domain name, you may do so at

http://privacyprotect.org/contact. We have a stringent abuse policy and any

complaint will be actioned within a short period of time.