UKIE Policy Paper:

Response to Ofcom site blocking Review

April 2011

ukie

THE ASSOCIATION FOR UK INTERACTIVE ENTERTAINMENT

Introduction

The Association for UK Interactive Entertainment (UKIE) is the trade association that represents a wide range of businesses and organisations involved in the video games industry.

UKIE exists to ensure that our members have the right economic, political and social environment needed for this expanding industry to continue to thrive. UKIE's membership includes games publishers, developers and the academic institutions that support the industry. We represent the majority of the UK video games industry: in 2009 UKIE members were responsible for 97% of the games sold as physical products in the UK and UKIE is the only trade body in the UK to represent all the major console manufacturers (Nintendo, Microsoft and Sony).

In 2009, the UK was the largest games market in Europe, the Middle East and Africa and the third in the world after the US and Japan.[1] In recent years the Internet has played a vital role for our industry and has been the main driver in the rapid growth and development of online games. The 2010 Digital Entertainment Survey found that 47% of people play online games on a console and 60% play online games on a PC. Not only has online game play increased in the last year, but among 15-24 year olds playing games online is now more popular than downloading music or watching films online.[2] All the popularly available game console systems connect to and interact with the Internet and most games today include an Internet-related aspect.

The videogame industry now offers more new, innovative ways for consumers to experience its products online than any other industry. However, the realities of the digital online environment are that pirated content has become more readily available and easier to download. The unwelcome development and growth of online piracy is a major hindrance and discouragement to the provision or take-up of online videogame services, as well as being highly damaging to traditional physical goods business models.

Because copyright enforcement mechanisms against online piracy are lacking, piracy in the UK is growing exponentially. The scale of unlawful game downloads is now so great, that without an effective and cost efficient solution, the potential damage to the industry is substantial. With the digital revolution, videogames that have resulted from ground-breaking technological development, years of effort and investments of tens of millions of pounds can be illegally duplicated and distributed worldwide online almost instantaneously. It is now a regular occurrence for new video game software to be distributed for illegal download on the Internet within minutes of official release and, with increasing regularity, even prior to release. Casual infringements, consisting of otherwise law-abiding people downloading tens of millions of pirate copies of games every month, are now exacting a far greater toll on the industry than in the past.

UKIE broadly supports the measures set out in the Digital Economy Act (DEA) to tackle unlawful file sharing and strongly believes that introducing the possibility to block particular infringing sites, as anticipated by the DEA, is important to ensuring the success of the DEA in combating unlawful file sharing and other internet infringements. Whilst the measures set out in the DEA may seek to reduce illegal peer-to-peer activity, consumers will still have access to illegal content through other methods of pirate distribution, including one-click hosts.[3] Unlawful sharing of copyright works is therefore likely to remain, in spite of the DEA, if the availability of, and access to, major suppliers or facilitators of such infringement are not stemmed. Blocking this availability at source, i.e. from the virtual spaces that facilitate access to the private files, would constitute a major step forward towards curbing illegal file sharing and online piracy and towards making the DEA an overall success. In addition, this would help to protect consumers from unwittingly infringing copyright by accessing and using these sites, and it would ensure that the illegitimate players, the Internet's 'bad actors', were not able to thrive while legitimate UK businesses suffer.

UKIE welcomes the opportunity to contribute to Ofcom's review of the site blocking provisions contained in sections 17 and 18 of the Digital Economy Act, to ensure that the technical feasibility of site blocking is established before the Act's full implementation. It is clear that a range of site blocking technologies is available, some of which are already being used in the UK; the site blocking provisions in the Act can clearly work "in practice." Whilst UKIE's preference is for IP hybrid blocking, already used by many ISPs, we would urge Ofcom to keep all blocking options on the table and to bear in mind that the possibility of circumvention by site owners is not just cause to dismiss site blocking per se; the purpose of site blocking is to disrupt large scale illegal and commercial piracy operations that operate in other countries outside of the reach of local laws or legal actions, at considerable cost to the video games industry and to the UK economy. Site blocking should also drive consumers towards easier, legal alternatives, especially when site blocking is combined with an education campaign to increase awareness of the value of copyright and the range of legal means possible to access content. The video games industry is already leading in this regard and will continue to play its part, but it needs legislative action to back up its efforts.

[1] Technology Strategy Board, Creative Industries Technology Strategy 2009-2012

[2] Ofcom Communications Market Report, 2010

[3] A one-click host (also known as a "download hub") is a cyberlocker abused to engage in unlawful activity.

Is it possible for access to a site to be blocked by internet service providers?

Site blocking involves the blocking by an ISP of its subscribers' access to a specific site or sites pursuant to an order of a court. The precise scope of site blocking, in terms of which kinds of sites should or should not be blocked, and the conditions that must be satisfied before they can be blocked, will, of course, depend upon the courts, using sections 17 and 18 of the Digital Economy Act as a guide. However, UKIE appreciates Ofcom's concern to ensure technical measures to facilitate site blocking are available to complement the legislation.

> *"Site blocking is an important tool in combating unlawful file sharing and other internet infringements"*

Internet Service Providers (ISPs) can use a variety of technical measures to block subscriber access to sites. These includes URL blocking, DNS blocking and IP blocking, as well as Proxy and Hybrid Pass-By Filtering or blocking.

- **URL Blocking:** The most accurate and granular way to block access to any content online is through URL blocking or filtering. URL blocking involves the placing of an additional device or the reconfiguration of an existing device or router in an ISP's network, and is more effective for blocking a specific item on a domain, such as a webpage or a single image, rather than an entire site.

- **DNS Blocking:** DNS blocking uses an existing ISP network infrastructure. To perform DNS blocking, an ISP makes entries in the DNS servers under its control that prevent requests to those servers for a site's domain name from resolving to its correct IP address. Blocking traffic based on a domain name involves a two-step process: (1) query - make periodic 'forward lookup' DNS queries to obtain the IP address or addresses to which the target domain name currently points, and (2) block - apply and continuously update blocking rules for the obtained IP address.

- **IP Blocking:** Blocking access to sites via IP addresses also uses an existing network infrastructure. It has become a fairly routine aspect of the management of ISP networks and does not have any appreciable impact on network performance. IP blocking is typically done either through an Access Control List (ACL), which filters traffic based on source and destination IP addresses, or by routing unwanted traffic to a 'null0' interface where it is dropped, so called 'black hole' filtering.[4]

- **Proxy and Hybrid Pass-By Filtering:** ISPs can also use a more refined blocking method called proxy filtering (in which a list of blocked URLs is compared by a web proxy against incoming requests and, where necessary, re-directed to a block page), and also a variety of cheaper hybrid pass-by filtering systems, which only inspect traffic that is actually going to the IP addresses of target sites, and then subject this traffic to more detailed (URL based) filtering. These latter systems incorporate both traffic redirection and the use of web proxies, and are intended to be precise and inexpensive. (Another pass-by filtering method is called port mirroring (or 'Ethernet tap'), in which a copy of all outgoing traffic is made and examined for URLs, which are then checked against a blacklist. If a request is found to be for a target site, the filter sends a TCP/IP RST (reset) signal to the remote server that it should interrupt the connection - and then diverts the user to a page with an error message or a page that could carry an educational message).

Whilst each of the above methods has 'pros' and 'cons' depending on the type of blocking desired, it is nevertheless clear that it is possible for access to a site/sites to be blocked by ISPs. In fact, ISPs already use site blocking technologies to manage their networks. IP blocking, for example, is already a fairly routine aspect of the management of ISP networks, and does not have any appreciable impact on network performance.[5] And some ISPs already use a form of hybrid blocking, for example BT's CleanFeed.

UKIE urges Ofcom to consider all site blocking options available, including URL filtering, IP blocking and DNS filtering. However, UKIE believes there is particular merit in an IP hybrid pass-by filtering system, due to its technical sophistication (discussed at point 2 in relation to circumvention), and the fact that this system is already in use in some form in the UK.

[4] For example, see Cisco White Paper: Remotely triggered Black Hole Filtering – Destination Based and Source Based http://www.cisco.com/web/about/security/intelligence/blackhole.pdf

[5] Black hole filtering technology is used to block SPAM, for example

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?

All of the methods outlined at point 1 would have the intended effect of blocking an ISP's subscribers' access to a target site or sites. Nevertheless, there are ways in which site operators can attempt to circumvent blocking to allow determined users to continue to access such sites.

A pirate site can seek to evade IP blocking by obtaining a new IP address without changing their URL, or by making the same content available through a different IP address or addresses attached to the same server. Sites can also use a technique known as 'fast fluxing' that involves the rapid and automated changing of IP addresses, and that is often done using botnet technology to compromise users' machines and to use them as portals to the web server's content (the basic idea behind fast flux is to have numerous IP addresses associated with a single fully qualified domain name, where the IP addresses are swapped in and out with extremely high frequency, by changing DNS records every few minutes). It will be necessary, therefore, to create and maintain a monitoring program to catch such IP address changes. As these IP addresses do not, either directly or indirectly, relate to an identifiable person there should not be any processing of any personal data monitoring these IP address changes. However, we estimate that only a small proportion of determined and tech-savvy users will use such methods to continue to access these pirate sites.

> *"100% effectiveness should not be the litmus test for the introducition of preventative measures to protect the UK economy from huge economic loss"*

Because DNS blocking will stop a request for a domain name before it has been resolved to an IP address, it will continue to prevent access to a target site even if it has changed its IP address. DNS blocking, however, only stops requests for the specified domain name; it does not stop requests for parent domains or sibling sub-domains of the domain name. In addition, the operators of pirate sites may also use a range of methods to evade or interfere with DNS blocking, including: simply using an IP address as a URL; changing a portion of their domain name and promulgating the new name in links to their site in advertisements, search engines, forums or blogs; distributing a small browser plug-in or other piece of software to allow users to retrieve the IP addresses of their servers; using multiple URLs to point to the same IP address; mirroring their sites (although users will have to be informed of the mirror's URL or IP address).

A hybrid IP-URL system may be preferable, especially as a form of hybrid blocking is already in use in the UK and other cost-effective systems are commercially available.[6] However, the above again highlights the need for Ofcom to take a flexible approach to any technical measures it suggests. Whilst UKIE continues to favour an IP hybrid blocking system, all technical options should remain on the table.

When assessing how easy it is for site operators to circumvent blocking, one must not lose sight of the fact that ISPs can take additional measures to minimise the potential for circumvention.[7] Similarly, 100% effectiveness should not be the litmus test for the introduction of preventative measures to protect the UK economy from huge economic loss, whilst those engaged in illegal activity who contribute nothing to the economy continue to profit. As the UK Government stated in its February 2008 response to the European Commission's Communication on Content Online, filtering measures (which can include site blocking) 'may well be part of any solution but they are unlikely to offer a panacea'. Site blocking, instead, should be regarded as an effective additional measure against online piracy and, in particular but not exclusively, against large scale illegal and commercial piracy operations that operate in other countries outside of the reach of local laws or legal actions. Even if site operators may be able to circumvent blocking, the blocking itself should still cause them very considerable inconvenience and loss of business. The time and expense of constant IP address switches, and the need to notify users of new addresses, should make the illegal activities of these sites less profitable and, therefore, also less prevalent. Similarly, sites hosting or linking to pirated content can and do generate significant amounts of revenue from online advertising and sales, and blocking them will cause their operators very considerable inconvenience and loss of business.

In addition one should not lose sight of another key aim of the site blocking measures: to drive consumers towards legal sites. Site blocking will simply make it too difficult and frustrating for the average consumer to access content from pirate sites. This is especially so since rights holders are likely to have the main popular pirate sites in common. These sites can be targeted simultaneously (and will therefore initially make it easier for ISPs to implement), so users will not be able to switch between the most popular and prolific sites to continue infringing.

There are a number of different types of circumvention tools that allow users to bypass site blocking or filtering: simple web proxies, virtual private network (VPN) services, open HTTP/SOCKS proxies and blocking-resistant tools. All of these tools use the same basic method to bypass blocking or filtering: they proxy connections through third party sites that are not blocked/filtered themselves. Some of the tools (just like pirate sites) can also use simple forms of blocking resistance to evade filtering - for example, a simple web proxy might maintain a list of alternative domain names to send to users in case one or more of its existing domain names is blocked. Blocking-resistant tools (such as Tor, which was initially developed as an anonymity tool, but is

[6] For example, BT's CleanFeed system or NetClean's Whitebox.
[7] For example a monitoring programme to catch IP address changes .

also effective as a circumvention tool) implement much more sophisticated methods to evade blocking.

The use of anonymous proxy services or anonymisers by Internet users will circumvent both IP and DNS blocking (and URL blocking as well). The filter will see only the URL or IP address of the anonymiser, not that of the requested site and will therefore not act to block access to the site unless, of course, the anonymiser is also blocked. Users may also be able to access mirrors of blocked sites, unless the mirror sites have also been blocked. Users attempting to evade a DNS filter can do so by manually entering the IP address for a DNS server not controlled by their ISP, or, of course, the actual IP address of the target site itself. Users can also run their own domain name server or resolver, but third-party public DNS servers are now widely available. For Internet users, pointing DNS requests to these unfiltered servers is simply a matter of updating a single parameter in their operating systems' Internet settings. Determined users who want to continue to engage in infringement are, therefore, able to route their traffic around DNS providers that enforce a site block.
Yet despite the wide availability and relative ease of many circumvention methods, we do not believe that the majority of ordinary Internet users will actually use them, either out of ignorance of the technologies, or out of fear for the possible consequences and risks. One of the key findings of a recent study[8] entitled '2010 Circumvention Tool Usage Report' by the Berkman Center for Internet and Society at Harvard University was that overall usage of filtering circumvention tools in countries with substantial national Internet filtering (such as China, Iran, Egypt and Burma) is very small (less than 3%) in proportion to the total number of Internet users. As the study itself concludes, the relatively small usage of circumvention tools, even in 'filtering countries', suggests either that users do not know that the tools exist, do not know how to find them, or consider that the benefits of using them do not outweigh the costs. IP and DNS blocking used in Italy against The Pirate Bay, for example, saw the audience drop by 600,000 in just 2 months.[9] Put simply, the technological circumvention of site blocking measures is not something that we believe most ordinary home users are likely to do. It requires knowledge that it is possible, an understanding of how to accomplish it (even if it is fairly easy), knowledge of the IP address of an alternate DNS server, and knowledge of the steps that must be taken to enter that IP address into the user's computer. Consumers want an easy, quick system for accessing content. Site blocking will inevitably make this a lot more difficult, and will drive consumers towards legitimate content.

Furthermore site blocking will be combined with education about the value of copyright and the damaging impact that piracy has on all creative, intellectual property based industries in terms of jobs, future prosperity, growth and innovation. This will raise both awareness and moral consciousness regarding the access of pirated – and increasingly harder to access – content, versus legitimate content. The video games and interactive entertainment industry is already playing a role in this regard. For example, UKIE is engaged with the Industry Trust to work on raising consumer awareness of the Digital Economy Act, including raising awareness of the importance of copyright and the promotion of legal online services. Similarly, the website www.jointhecteam.com represents an effort by game publishers to create curriculum for school teachers and school librarians to use in introducing IP concepts to children. Although the site is geared towards American educators, its curriculum and IP education lessons are universal. These efforts, combined with difficulty reaching illegal content together with the easy accessibility of legal content will all help ensure circumvention by users is at a minimum.

600,000

Pirate Bay audience drop in Italy following introduction of IP and DNS blocking

3. What measures might be adopted by internet service providers to prevent such circumvention?

As noted at point 2, it may be possible for site operators to circumvent site blocking measures. However their ability – or at very least the ease – with which they may be able to circumvent blocking will depend on the type of site blocking technology employed by ISPs. ISPs can also adopt measures to prevent circumvention. For example, ISPs will need to create and maintain a monitoring program to catch IP address changes used by sites to evade IP blocking. While site operators will likely take measures to evade or circumvent the blocking of their sites, site blocking will, at a minimum, still cause them considerable inconvenience and loss of business.

[8] http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/2010_Circumvention_Tool_Usage_Report.pdf
[9] International Federation of the Phonographic Industry

4. How granular can blocking be – i.e. can specific parts of the site be blocked, how precise can this be, and how effective?

The granularity of blocking is dependent on the blocking measure used. For example, there are two types of IP filtering which differ in their granularity and resource consumption: layer 3 and layer 4 filtering. Layer 4 filtering can use the destination port number to allow blocking based on a particular service. This type of filtering can block access to a particular web site while allowing access to email, chat and other services run from the blocked host server.

The most accurate and granular way to block access to any content online is through URL blocking or filtering. URL blocking, however, involves the placing of an additional device or the reconfiguration of an existing device or router in an ISP's network, and is more appropriate for blocking a specific item on a domain, such as a web page or a single image, rather than an entire site.

> *"The purpose of sections 17 and 18 is to allow the courts to block specific sites after an injuction has been sought"*

A hybrid blocking system that would only inspect traffic that is actually going to target IP addresses or IP address ranges, and then subject this traffic to more detailed (URL based) filtering would be highly granular and accurate. In terms of granularity, proxy and hybrid filtering approaches provide the greatest flexibility, allowing blocking both by full webpage URL and by webpage content. Hybrid pass-by filtering systems have the advantages of IP blocking without the risks of over-blocking, and the advantages of URL blocking without the need for significant filtering resources. At this present time, UKIE would urge Ofcom to keep all blocking options on the table, mindful of UKIE's preference for IP hybrid blocking, already used by many ISPs.

5. How effective are sections 17 and 18 of the Act in providing for an appropriate method of generating lists of sites to be blocked?

The purpose of Sections 17 and 18 is not to provide a method of generating lists of sites to be blocked but rather to provide for the Secretary of State to 'make provision about the granting by a court of a blocking injunction in respect of a location on the internet which the court is satisfied has been, is being or is likely to be used for or in connection with an activity that infringes copyright' and is '(a) a location from which a substantial amount of material has been, is being or is likely to be obtained in infringement of copyright, (b) a location at which a substantial amount of material has been, is being or is likely to be made available in infringement of copyright, or (c) a location which has been, is being or is likely to be used to facilitate access to a location within paragraph (a) or (b).' In other words, the purpose of sections 17 and 18 is to allow the courts to block specific sites after an injunction has been sought. No list of sites needs to be generated for this purpose, although UKIE would be happy to work with Ofcom and/or with ISPs to identify a list of egregious sites we would seek to block under the Act.

Of course, there is nothing in Section 17 that would prevent a rights holder from seeking a blocking injunction against a number of sites, but that is very different to the generation of a list of sites to be blocked. Similarly, whilst sections 17 and 18 do not in and of themselves provide for lists of sites to be blocked, they could be very effective in this regard. If the process of applying for blocking injunctions is relatively straightforward and cost effective then it is likely that rights holders will avail of the site blocking provisions in sufficient numbers and with sufficient regularity to "generate a list of sites to be blocked". This "list" would be the cumulative and ever-evolving result of successful rights holder applications for blocking injunctions. Again though, the DEA does not provide for or contemplate any other kind of site blocking list, and it doesn't need to in order to provide an effective site blocking regime in the UK.

6. If possible, identify either a potential range of costs for ISP blocking solutions or the main drivers of those costs.

The costs of site blocking for ISPs are generally considered to be low, and relevant technologies are offered by a number of third party vendors, should an ISP not be able to engage in such blocking itself. ISP costs are associated with the procurement, implementation and ongoing operation and management of a blocking or filtering solution. The actual costs will, of course, depend upon the blocking method chosen and on the size of the ISP and how it delivers its services (e.g., network size and architecture).

The cost components associated with the implementation of blocking may include the purchase costs of any necessary hardware and software (if not already owned by the ISP) or specific adaptation costs required for existing systems, installation and configuration costs associated with the implementation of the solution, and network reconfiguration costs associated with the re-arrangement of the ISP's network to accommodate the solution (e.g., redirecting user traffic flows). After blocking is implemented, and depending on the solution chosen, ISPs may also incur a range of costs associated with the ongoing operation, maintenance and management of the blocking solution.

Analysis of the costs associated with site blocking/filtering appears to suggest that the cost per user reduces with ISP size. This arises from economies of scale and discounting arrangements that tend to favour larger ISPs. For small ISPs, third party hosted filtering services may be an option.

DNS blocking is very inexpensive as recursive resolvers do not need to respond particularly quickly and existing configuration options in DNS servers can be used to implement filtering. HTTP proxies require connections to be built by reassembling the constituent packets - which does require substantial resources. Hybrid HTTP proxies are more complex to set up, but once this is done, they are only slightly more expensive than IP filtering, despite their much higher versatility. This is because the HTTP proxy receives only a small proportion of the traffic, and so does not need to be particularly powerful.

IP blocking is likely to be the cheapest option available and does not require additional infrastructure or equipment within an ISPs network. Nevertheless, hybrid blocking can also be a cost effective solution, particularly in the UK where use of hybrid systems is considered to be fairly well advanced. "Cleanfeed", for example, is already used by BT. NetClean, which sells the Whitebox system, is estimated to cost E10,000 per box, and a typical install would be two boxes. The cost to subscribers would therefore be equally low, at just six pence.[10] Whilst there are other systems commercially available, NetClean's Whitebox is already in use in the UK, and is proven to be effective in jurisdictions such as Norway andNew Zealand. And, if not already in use, large ISPs will have various ways of implementing a cleanfeed solution already. Additional capacity will just be needed to handle extra sites, which is not a technical but a commercial/resource issue.

[10] Based on estimates of 10 cents per subscriber. Prices are an estimate and would of course be subject to commercial negotiation

List of UKIE members

Full members

4mm Games
505 Games Ltd
Activision Blizzard UK Ltd
Atari EU
Avanquest Software Publishing Ltd
CE Europe Ltd
ChangYou.com (UK) Company Ltd
Codemasters Ltd
Disney Interactive Studios UK
Easy Interactive
Electronic Arts Ltd
Focus Multimedia Ltd
Kalypso Media UK Ltd
Koch Media Ltd
Konami
Licensed 4 U Ltd
Majesco Europe Ltd
Mastertronic Group Ltd
Mediatonic Ltd
Microsoft Ltd
Midas Interactive Entertainment Ltd
Namco Bandai Partners UK Ltd
NCsoft Ltd
Nintendo UK Ltd
Nordic Games Publishing AB
Piggyback Interactive Ltd
Playdom Inc.
Rising Star Games Ltd
SEGA Europe Ltd
Sony Computer Entertainment Europe Ltd
Square Enix Ltd
Take2 Interactive Software Europe Ltd
Tecmo Koei Europe Ltd
The Stationery Office Ltd
THQ International Ltd
Tradewest Games Ltd
Trion Worlds Europe Ltd
Ubisoft Ltd
Warner Bros Interactive Entertainment
White Room Games Ltd
Zenimax Europe Ltd / Bethesda Softworks Europe Ltd

Associate Members

AGI World Ltd
AIME Ltd
ASP Solutions Ltd
Casual Games Association
CD Team Ltd
Centresoft Ltd
Channel Four Television Company Ltd
Eurogamer Network Ltd
Fidelity Investment Services Ltd
Future Publishing Ltd
GameHorizon
GAME Stores Group Ltd
Harbottle & lewis LLP
Hasbro Europe
Intent Media Ltd
Internet Advertising Bureau
OK Media Ltd
Pqube Ltd
Sony DADC UK Ltd
Target Media Ltd
VGM
Virgin Media Ltd

Academic Members

De Montfort University
National Film & Television School
Ravensbourne College
Sheffield Hallam University
Teeside University - School of Computing
University of Abertay Dundee
University of Glamorgan - Cardiff School of Creative & Cultural Industries
University of Hull
University of Wales, Newport (Skillset Media Academy Wales)