



Analysis

UK: Internet censorship looms as government finds alternatives to flawed Digital Economy Act

Max Rowlands

Introduction

A July 2011 High Court judgement has paved the way for the routine blocking of websites accused of infringing copyright. In a landmark test case of the Copyright, Designs and Patents Act (CDPA), for the first time in the UK a judge ruled that an internet service provider (ISP) must stop its subscribers accessing a website. The establishment of this legal precedent has allowed the government to abandon the website blocking provisions of the Digital Economy Act (DEA), which have proven to be poorly drafted and difficult to implement, without drawing the ire of creative industry copyright holders who lobbied fervently for its introduction. A slew of cases against websites are now expected to be brought under the CDPA. A voluntary code for blocking websites could also be introduced at the behest of culture minister Ed Vaizey who has held a series of secret meetings with ISPs and copyright holders over the last six months.

The government believes that website blocking together with the DEA's copyright protection scheme - under which the government would be able to suspend the internet connections of individuals accused of persistent copyright infringement if they fail to react to warning letters - will lead to a hefty reduction in the amount of copyrighted content being distributed online, saving the UK's creative industries around £200 million each year. But the accuracy of this figure has been questioned, and the government has been accused of giving too much consideration to the interests of major corporations to the detriment of ISPs and their subscribers. Critics argue that the measures are a costly,

disproportionate and heavy-handed response that will punish and criminalise individuals outside the remit of the judicial system. This forms part of a much wider European debate about online censorship and the right to access the internet. Across Europe, website blocking is increasingly being held up by governments as a cure for all ills, be it pornography, copyright infringement, or religious extremism. In reality, the practice tends to treat the symptom rather than the cause, and can be easily bypassed.

Background to the DEA

The Digital Economy Bill was rushed through parliament in April 2010 during the 'wash-up' - a period of parliamentary limbo when the date of a general election has been set and the House of Commons is soon to be dissolved. At this undemocratic juncture, due process is replaced by horse-trading between the whips of political parties as deals are hammered out and rushed through parliament with minimal scrutiny. The Digital Economy Bill was debated by just 20 people in the House of Commons before being added to the statute books. Speaking at the time, Liberal Democrat leader Nick Clegg castigated the manner in which the legislation was "rammed through parliament at the last minute... [its passage is] a classic example of what's wrong with Westminster." The Bill was one of the most heavily lobbied pieces of legislation in UK parliamentary history. Lord Puttnam said: "We have been subjected to an extraordinary degree of lobbying...The lobbying process that has gone into this Bill has been quite destructive and has done none of us very much help at all." [1] ISPs, major

internet companies such as Google and Yahoo, consumer organisations, and NGOs all voiced serious misgivings about sections 3 to 18 of the Bill but were given short shrift.

DEA sections 3 to 18

Sections 3 to 16 create a system to punish internet users believed to be guilty of online copyright infringement. Copyright holders can send an ISP a list of IP addresses belonging to users they believe to have unlawfully downloaded their content, along with details of the alleged infringement, in the form of a “copyright infringement report”. If there is sufficient evidence, the ISP would then be obliged to determine which of their subscribers used the IP address at the time of the alleged infringement, and send them a warning letter. If a subscriber continues to commit infringements they will be sent warning letters until they reach a threshold at which point they will have their IP address added to a “copyright infringement list.” People on this list will be open to two forms of punitive action. Copyright holders can access this list of repeat offenders, and can apply for a court order to force ISPs to reveal the name and address of the subscriber tied to each IP address. With this information they could then instigate legal proceedings for civil copyright infringement. Additionally, individuals on the “copyright infringement list” can have their internet connection limited or suspended entirely by the Secretary of State.

Sections 17 and 18 of the DEA establish guidelines for the creation of new regulations to restrict access to “locations on the internet.” The Home Secretary will be able to apply for a court order to block access to websites that either make available or facilitate access to a “substantial amount of material...in infringement of copyright.”[2] Section 17 stipulates that the court must take into account, among other things, the importance of freedom of expression and any evidence presented of steps taken by ISPs or the website’s owner to prevent copyright infringement, and steps taken by the copyright holder to facilitate lawful access to their content.

Although the DEA came into force on 8 June 2010, sections 3 to 18 have yet to come into effect. There are two main reasons for this. Firstly, the Act provides only a framework for how its copyright protection systems should be implemented. Ofcom, the independent regulator and competition authority for the UK communications industries, is responsible for drawing up regulatory codes to govern how the new schemes will operate. These have to be adopted by parliament as secondary legislation in the form of statutory instruments. This has proven to be no easy

task because, as the current government readily acknowledges, the DEA is badly drafted. In March 2011, culture secretary Jeremy Hunt told parliament:

We are also working hard to implement the Digital Economy Act, as we think the principles behind it are important, but it is very difficult to implement because many of its measures did not get proper parliamentary scrutiny as the hon. Gentleman’s discredited Labour Government rushed it through Parliament in their final dying days.[3]

Secondly, the legality of sections 3 to 18 has been challenged by ISPs in the High Court. In November 2010, this forced the government to suspend their implementation indefinitely.

The role of Ofcom

Sections 3 to 7 of the Act provide guidelines for the drafting of an “initial obligations code.” It will govern how the new letter-based copyright infringement system works and clearly define the obligations of copyright holders and ISPs. Ofcom published a draft code in May 2010 that was heavily criticised for not adhering to the Act’s framework and for leaving key questions of functionality unresolved. Perhaps the most important of which is: what level of evidence must a copyright holder be required to produce against an individual before their ISP sends them a warning letter?

Ofcom must also produce a “cost sharing order” to determine how the price of operating the system should be split between copyright holders and ISPs. The draft code stipulates that copyright holders should pay 75 per cent of the system’s costs, with ISPs liable for the remaining 25 per cent.

Under the terms of the EU Technical Standards Directive, both codes need to be approved by the European Commission.[4] This will cause further delays, particularly because the government was initially unaware that the ‘cost sharing regulation’ needs EU approval.[5]

Drafting the codes has been a problematic and costly process. In June 2011, a freedom of information request revealed that the cost of Ofcom investigations into the practicability of the DEA will reach £5.9 million - although copyright holders and ISPs are due to pay this money back when sections 3 to 18 are implemented.[6] The ‘initial obligations code’ that was scheduled to be finalised by January 2011 will not be introduced before spring 2012 at the earliest.

Judicial review

The delay in finalising the codes is largely because, on 10 November 2010, BT and TalkTalk, the UK's two largest ISPs, won the right to a judicial review of sections 3 to 18. They argued that the Act infringes internet users' "basic rights and freedoms" and that it was subjected to "insufficient scrutiny" by parliament. They were also financially motivated - Ofcom's draft initial obligations code of practice stipulated that only ISPs with over 400,000 subscribers would be obliged to participate in the new copyright infringement scheme. BT and TalkTalk argued that this would put them at an unfair business disadvantage because some of their customers might choose to join smaller ISPs in order to avoid being monitored. They also objected to having to contribute to the administrative costs of a system that does not benefit them or their subscribers. BT also claimed to be fearful of "investing tens of millions of pounds in new systems and processes only to find later that the Act is unenforceable." [7]

The High Court granted the judicial review on all four of their contested legal points, namely: that the European Commission was not given enough time to scrutinise the Act; that the Act does not comply with EU privacy laws; that the Act does not comply with EU e-commerce laws; and that the Act's provisions are "disproportionate" because they infringe, among other things, rights to privacy and freedom of expression afforded by the UK Human Rights Act and the free movement of services provided for by the Treaty on the Functioning of the European Union. [8]

On 20 April 2011, the High Court ruled against all of these points. [9] However, Justice Kenneth Parker did uphold part of the cost-sharing objection which means that ISPs will not have to pay for the creation and administration of an appeals body. BT and TalkTalk sought permission to appeal the High Court's decision but on 21 June this was refused.

Critical reports

In May 2011, the legality of the Act was also challenged by the United Nations Human Rights Council. A report written by Frank La Rue, UN special rapporteur on the promotion and protection of the right to freedom of opinion and expression, directly contradicts the high court's judicial review judgement. La Rue argues that blocking websites and suspending people's access to the internet would violate article 19 of the Universal Declaration of Human Rights which provides the "right to freedom of opinion and expression." He also warned against delegating power to private companies and

emphasised the need for transparent judicial oversight. La Rue proposes that sections 3 to 18 be amended or scrapped:

The Special Rapporteur calls upon all States to ensure that Internet access is maintained at all times...the Special Rapporteur urges States to repeal or amend existing intellectual copyright laws which permit users to be disconnected from Internet access, and to refrain from adopting such laws. [10]

A July 2011 study by the Organization for Security and Co-operation in Europe concurs, arguing that access to the internet is now a basic human right because it has become an indispensable means of taking part in cultural, social and political discourse:

Everyone should have a right to participate in the information society and states have a responsibility to ensure citizens' access to the Internet is guaranteed. [11]

On 14 June 2011, Liberal Democrat MP Julian Huppert sponsored an early day motion in the House of Commons. He argued that in light of the UN report the government should urgently review sections 3 to 18 of the DEA. By 22 July 2011, 109 MPs had signed the motion. [12]

DEA sections 3 to 16: the copyright infringement scheme

Despite these concerns, the government has indicated that it hopes to begin sending out copyright infringement letters by early 2012. The scheme has been criticised for both practical and ethical reasons. Andrew Heaney, TalkTalk's executive strategy director, described the DEA as a "dog of a bill" that is backwards-looking and doomed to fail:

The world has changed through the internet, and you can't stop people sharing music and films. You can't police the internet like you can police bootleg CDs at a car boot sale. This act is trying to solve yesterday's problem...There are two things you can do to make people pay. One is to educate them, and make them aware that copyright infringement is not a victimless crime - that if they don't pay, then film, music and books just won't be as good. The second is to support innovative, attractive paid services, such as Apple's iTunes store. The emphasis has to be on the carrot and not on the stick. All this act does is try to sustain the old, arcane way of doing things. [13]

The scheme's biggest technical problem is that it

relies on an IP address alone as a means of identifying illegal downloaders. There are a number of ways in which internet users can mask their IP address to avoid being tracked. The DEA will make determined copyright infringers more cautious and will encourage the development of new methods of file-sharing that offer greater anonymity to its users. Giving evidence to the judicial review of the DEA, Dr Richard Clayton, an “internet expert” and “special advisor” to parliamentary select committees, left little doubt as to the unsuitability of the DEA’s detection methods:

Academic researchers at the University of Washington were running specialist Bit Torrent programs that looked as if they were doing file sharing, but were actually just recording statistics about the speed and effectiveness of the system. They received a number of ‘cease-and-desist’ letters from copyright owners who were under the impression that because the tracker machine had registered their interest in a particular file they were transferring the file.

This might have remained an edge case of little practical interest, since of course almost everyone else whose IP address was present in the tracker file was actively file sharing. However, the researcher found that they could forge entries in the torrent files, giving IP addresses that were not involved in file sharing at all: most famously they ‘framed’ their network-connected laser printer, which duly received a cease-and-desist letter.

I understand that it is now commonplace for trackers to add forged entries themselves, making this data useless for evidentiary purposes - albeit at the cost of slightly degrading the effectiveness of the file sharing network.

Similar issues arise with other peer-to-peer systems, making reliance on identifying the participants during the search phases extremely problematic.[14]

Further, tracing unlawful file-sharing to an IP address does not tell you which person committed the infringement. An IP can easily be spoofed, and the widespread use of wireless technology means that access to internet connections is often insecure. In August 2010, a study found that roughly a third of London households have “wifi networks that can be hacked with ease.”[15] To determine culpability the police would need to seize and forensically examine every household computer. This is standard practice in child pornography investigations, but would be totally impractical here.

Although any number of people can share access to an IP address, only the account holder will be sent a copyright infringement letter. Innocent people are sure to be targeted for the behaviour of others. Crucially, the account holder is not legally responsible for all internet traffic tied to their IP address. They are only liable for copyright infringements made using their internet connection if they carried out the infringement themselves or authorised someone else to do so. If they did neither of these, they can simply inform their ISP that they have no case to answer.

This means that copyright holders are likely to have difficulty securing convictions against account holders on the basis of evidence collected under the DEA. Worryingly, the possibility exists that copyright holders will instead turn to the lucrative practice of ‘speculative invoicing’ - an industry that has grown up around extorting money from suspected file-sharers.[16] UK law firms acting on behalf of copyright holders are able to compel ISPs to hand over the personal details of their subscribers through a Norwich Pharmacal order in the High Court - precisely the same method as would be used under the DEA.[17] These firms acquire as many names and addresses of suspected copyright infringers as possible and send out letters indiscriminately, informing the recipient of their wrong doing, requesting monetary compensation and threatening legal action if they do not comply. They have no intention of taking cases to court but enough people are scared into paying up to make the practice immensely profitable. The DEA could easily be used to fuel this industry.

While there is uncertainty over how subscriber details might be used by copyright holders, the ramifications of limiting or disconnecting individuals from the internet at the behest of the Secretary of State are far more tangible. This is a blanket measure that will affect anyone who uses the internet connection in question. It thus has the potential to criminalise and stigmatise whole families. Giving evidence to the judicial review of the DEA, Jim Killock, director of the Open Rights Group, also warned of the chilling effect the Act will have on the provision of public internet access. Organisations and businesses including libraries, schools, pubs and restaurants have all expressed concern about the possibility of being held liable for the internet activity of members of the public.

The Digital Economy Act will see these institutions facing costly and overly burdensome requirements to control access to their connections. This is particularly worrying if it leads to a withdrawal of these services because internet use outside the

home has become an important piece of the supporting infrastructure of the networked world.[18]

Clearly, having one's name added to the "copyright infringement list" can have severe consequences. Given this, and the fact that relying on IP addresses alone as a means of identifying individuals responsible for copyright infringement is intrinsically problematic, it is extremely worrying that Ofcom indicated in its draft "initial obligations code" that it will place responsibility for verifying the accuracy of evidence in the hands of copyright holders and ISPs. There would be no independent oversight, and no threat of sanctions should mistakes be made. The Open Rights Group asks: "how is anyone meant to trust this code if we can't see how the evidence is gathered or checked?" Graham Hann, media and technology partner at law firm Taylor Wessing, warned *The Guardian* that:

...the DEA could effectively require ISPs to be judge and jury. How is an ISP to know whether a reported incident is in fact an infringement? In practice ISPs are likely to be forced to treat all reports as valid, giving significant power to rights holders. 19

Allowing copyright holders and ISPs to self-regulate the new system would afford them an inordinate amount of power. When the DEA was passed, Nick Clegg bemoaned the fact that "it was far too heavily weighted in favour of the big corporations," and this is becoming increasingly clear. The Act benefits neither ISPs nor their subscribers. If ISPs are forced to pay 25 per cent of the administrative costs of sending infringement notification letters, this financial burden is likely to be passed on in full to their customers. In February 2011, the House of Lords Merits of Statutory Instruments Committee published its twenty-first report in which it expressed concern that the effect of this could be to price some people out of broadband internet connections. Incredibly, the government admits that this is likely to be the case, but argues that the ends justify the means:

The Government says that they have acknowledged that there may be an effect on broadband take-up should ISPs pass on the full cost of the process, but although this is regrettable it needs to be balanced against the wider benefit to the UK's digital economy.[20]

The Government claims that unlawful file-sharing costs the creative industries £400 million in lost revenue each year. The DEA, it contends, would result in an annual increase in revenue for copyright holders of £200 million a year because 70% of people

sent a warning letter would stop infringing. The accuracy of these figures has been widely disputed. In the course of the Act's judicial review, TalkTalk's lawyers stated that peer to peer file sharing covered by the DEA accounts for less than 40 per cent of all online infringements. The notion that 70% of letter recipients would stop infringing was also dismissed as "naïve and optimistic" - the judge agreed that it is difficult to predict how people would respond.[21]

Estimates of the DEA's financial benefit to the creative industry are based on the erroneous assumption that a reduction in file sharing will result in a proportionate increase in revenue for copyright holders. The music industry in particular, represented by the British Phonographic Industry, claims to be suffering huge losses at the hands of illegal-downloaders - a figure of £200 million was quoted in 2009.[22] But the UK computer gaming industry is thriving, and in 2009 the UK film industry had its best year in almost three decades. The entertainment industry has changed rapidly since broadband became widely available, becoming increasingly diverse and competitive. Consumers have more ways than ever in which to spend their money. As Steve Lawson, a musician and member of the Musicians Union who campaigned against the Act, says:

The figures quoted for industry 'losses' are...utterly nonsensical if mapped against spending trends on 'physical and download entertainment media' - we are part of a much bigger entertainment industry now than we ever were, and we don't dominate it in the way we did from 1956 to 1998. Games and DVD are a bigger part of it than ever. And entertainment spending continues to rise. So 200 million hasn't been 'lost', it's being spent elsewhere.[23]

Further, the figures used by the government to justify the DEA were supplied to them by the very corporations who stand to benefit from its implementation - a clear conflict of interest. The Open Rights Group claims that the Act's impact assessment cherry-picks research and ignores reports that estimate a lower impact on revenue. The report on the music industry is cited only as "Jupiter 2007" and has not been made available to the public.[24] In March 2011, an LSE study poured scorn on the notion that illegal-downloading is the chief cause of the music industry's financial decline.[25]

The "wider benefit to the UK's economy" that supposedly justifies the negative financial impact of the Act on ISPs and its subscribers is dubious. According to the Open Rights Group:

It does not seem immediately acceptable to balance the costs to ISPs and their poorest customers ability to access the Internet against this kind of flawed and narrow evidence. We need full details of the analysis behind these figures.[26]

TalkTalk's submission to the Merits of Statutory Instruments Committee states that: "The Government's procedure that culminated in the making of this [cost sharing] Order was (and remains) deficient." It argued strongly that ISPs should not have to foot 25 per cent of the bill for administering the new system because:

The obligations raise issues of legal importance since they are, in several respects, incompatible with the [EU] Authorisation Directive.

The obligations give rise to public policy concerns since they are unreasonable and not justifiable because they require ISPs to incur costs even though they receive no benefit. Further, the obligations will distort competition and result in inefficiency.[27]

In its current form, Ofcom's cost sharing order is almost certain to fall foul of the EU Authorisation Directive (2002/20/EC) which stipulates that communications service providers should be subject to minimal government regulation.[28] The Directive's Annex provides a list of conditions under which regulation is justifiable, none of which cover the establishment of a system in which charges are levied on ISPs for the sole benefit of copyright holders. In January 2011, the European Commission voiced this concern in its comments on the draft cost sharing order, and asked for clarification. The Commission questioned both whether the charges ISPs would be required to pay complied with the Directive's definition of "administrative costs," and whether they could be considered to be "objective" given "Internet Service Providers do not appear to benefit in any way from the planned online copyright measures." [29]

As previously mentioned, the High Court has since ruled that ISPs should not have to contribute towards the administration of an appeals body, but they will still be expected to foot 25 per cent of the bill of sending copyright infringement letters to subscribers. If the cost-sharing arrangements of the DEA fall foul of EU law, the passage of the more contentious "initial obligations code" is likely to be treacherous.

DEA sections 17 and 18: website blocking

In February 2011, culture secretary Jeremy Hunt asked Ofcom to review the DEA's website blocking powers. He made it clear that he had "no problem with the principle of blocking access to websites" but wanted to be sure that sections 17 and 18 were practicable. Just as identifying copyright infringers by IP address alone is inherently problematic, there are deep-rooted technical difficulties with blocking access to websites. Richard Clayton highlights the fact that the Internet Watch Foundation's blocks on child pornography websites are easy to evade. A website's operators can switch to an unusual port number or encrypt their traffic, while users can reroute their web traffic through a different IP address in a foreign country that is unaffected by the blocking. "Anonymous proxies" are freely available and already commonly used by UK internet users to avoid website restrictions imposed in the workplace or at school. Clayton concludes that "the main impact of any attempt to use blocking systems to prevent unlawful file sharing would be to bring evasion techniques into everyday parlance":

If evading blocking of access to child sexual abuse image websites is so straightforward, for an activity that people might find hard to discuss with friends, imagine how quickly knowledge would spread about how to detect and evade blocks on such a widely indulged in activity as unlawful file sharing.[30]

Hunt's decision to review sections 17 and 18 engendered optimism among some critics of the Act that the government was taking their concerns seriously, but within a matter of weeks *The Guardian* revealed that culture minister Ed Vaizey had begun meeting with copyright holders and ISPs in secret to draw up an alternative voluntary code for blocking websites.[31] A voluntary code is intrinsically more worrying because it does not require parliamentary approval and there is no telling how much regulatory oversight, if any, it will include.

Vaizey is taking his cue from the USA, telling the Intellect 2011 Consumer Electronics Conference: "There are rumours of a voluntary system being implemented in the US and that would be a significant game-changer." [32] He is also showing increasing annoyance with the attitude of ISPs - he told the conference that he found "their attitude odd" and the BPI annual general meeting: "It would be nice if BT put as much effort into creating a fantastic music offering for its customers as it does trying to overturn an Act of Parliament." [33]

BT, TalkTalk, Universal Music, the BPI and Google

representatives attended the initial secret discussions. No consumer organisations were invited. *The Guardian* reported that they agreed to form a working group in order to find “a plan B, or at least a plan that works alongside section 17 which would be the legal backstop.” This working group convened several times over the following months and only at a meeting held on 15 June was a consumer organisation, Consumer Focus, invited to attend.

The government’s decision to formulate public policy in closed meetings with groups who represent a narrow range of commercial interests is clearly undemocratic. Website blocking is an issue of censorship that will affect all internet users and therefore requires a full and open debate. Moreover, the previous government’s decision to ignore the concerns of civil society and consumer groups when drafting the DEA is one of the main reasons it is poorly written and difficult to implement.

At the meeting on 15 June, copyright holders presented Ed Vaizey with an eight page draft proposal for a voluntary code of practice.[34] The new system would involve copyright holders submitting evidence to be evaluated by two independent bodies, a “council” and an “expert body,” who could then apply for a permanent injunction against a website from the Interim Applications Court that sits in the High Court. If an injunction is granted ISPs who have signed up to the code would block access to the site. Alarming, there would be “circumstances upon which a site qualifies for expedited court procedures.”[35] Further:

Evidence should also be submitted to show the urgency with which the measures are sought to inform any balance that needs to be struck by the expert body and the Court between the need for swift action and the need for sufficient evidence. (emphasis added)

This represents an alarming disregard for due process - prioritising quick action over legal thoroughness. What level of evidence will be required to block a website and will its owners be afforded an adequate opportunity to defend themselves? Internet copyright infringement appears to be a legal grey area and in many cases determining whether a website should be blocked will be highly contentious. It is also likely that there will be instances of entirely innocent websites being unjustly targeted. This was the case in June 2011 when Universal Music launched a scheme to stop “pirate” websites making money through advertising. Among the websites targeted were Vimeo (a video streaming website similar to

YouTube), the Internet Archive, BitTorrent’s corporate page, and a number of music blogs that, ironically, Universal Music depends on to promote its recording artists.[36]

If a website is blocked it will automatically be associated with illegality. This will have a stigmatising effect, damaging its public image and in some cases undermining the legitimacy of its content and money-making potential, regardless of whether the blocking is effective or subsequently removed. This makes it all the more important that the decision-making process is both scrupulous and transparent. Peter Bradwell, a copyright campaigner and member of ORG, argues that the scheme is dangerous because it allows “an industry such a direct role in deciding what content people can and cannot see and further establishes the infrastructure of censorship.”[37] Moreover, it fails to acknowledge the potentially damaging implications of web censorship on innovation and freedom of expression - something the copyright holder group behind the proposal appears to have ignored completely. Ground-breaking new websites could be stifled in their infancy - a website like YouTube would probably fall foul of the DEA’s provisions. Website blocking has serious consequences and should not be administered in an “expedited” manner.

Copyright, Designs and Patents Act section 97A

The draft proposal for a voluntary scheme called for the website blocking provisions of the DEA also to be implemented, allowing the two systems to run in tandem. But on 3 August 2011 business secretary Vince Cable announced that sections 17 and 18 would be scrapped. This decision was influenced by two things. Firstly, Ofcom published its report on the practicability of website blocking which concluded 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.[38]

Secondly, on 28 July 2011 six major Hollywood film studios, represented by the Motion Picture Association (MPA), won a landmark test case in the High Court to force BT to block access to the website Newzbin2 for allegedly infringing copyright. The case was brought under Section 97A of the Copyright,

Designs and Patents Act 1988 (CDPA), as amended by the Copyright and Related Rights Regulations 2003 which is the UK implementation of the European Union Copyright Directive (2001/29/EC). S97A gives the High Court the 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” (emphasis added). This is the first time the CDPA has been used in this way and the first time a UK judge has ruled that an ISP must block access to a website.

In court, BT had contended that an ISP’s role is merely that of an intermediary and as such it is not responsible for what its subscribers download, just as Royal Mail is not responsible for the contents of the packages it delivers. They argued that ISPs do not have “actual knowledge” of copyright infringements made by their subscribers and are therefore not obliged to prevent it. Justice Arnold disagreed:

In my judgment it follows that BT has actual knowledge of other persons using its service to infringe copyright: it knows that the users and operators of Newzbin2 infringe copyright on a large scale, and in particular infringe the copyrights of the Studios in large numbers of their films and television programmes, it knows that the users of Newzbin2 include BT subscribers, and it knows that those users use its service to receive infringing copies of copyright works made available to them by Newzbin2. For the reasons given above, that knowledge satisfies the requirements of section 97A.[39]

BT accepted the ruling, indicating that it has no intention to appeal, and will meet the MPA in court in October to determine precisely how the blocking will work. Their head of retail, Simon Milner, although “not deliriously happy” about the judgement, reflected that it at least “provides a level of clarity we’ve never had before.” He said that s97A shows that decisions over whether to block websites must be assessed and ruled on by a court of law and that BT would never restrict their subscribers’ internet access unless legally bound to do so. But there is no telling if other ISPs will be so scrupulous. Justice Arnold said:

The Studios have made it clear that this is a test case: if they are successful in obtaining an order against BT, then they intend to seek similar orders against all the other significant ISPs in the UK. The other ISPs were invited to intervene in the present application if they so wished, but have not done so.

This is unlikely to be necessary because, although the case brought by the MPA only applies to BT, the BBC reports that all major ISPs will act on the court’s decision and block access to Newzbin2.[40] It is expected that many more websites suspected of infringing copyright will now be targeted. BPI chief executive Geoff Taylor said in reaction to the judgement: “We will use the decision as appropriate in our strategy going forward.”[41]

Loz Kaye, leader of Pirate Party UK which campaigns for digital rights, said “The wording of the judgment leaves no doubt that property rights of creators trump those of human rights and free expression” and predicted that the blocking will be ineffective: “Other sites will pop up, it looks like we are doomed to a perpetual round of legal whack-a-mole.”[42] Similarly, digital rights campaigner Milena Popova in an article in the Open Rights Group magazine argued that Justice Arnold had “taken the broadest possible interpretation of Section 97A” and warned that it could prove to be more damaging than the website blocking provisions of the DEA:

[Section 17 and 18] speak of proportionate responses and infringement activities that have a “serious adverse effect on businesses or consumers” and explicitly state that in determining whether to grant an injunction the court must consider the importance of freedom of expression. No such formal safeguards are to be found in Section 97A. Ironically, BT’s counsel used Section 17 of the Digital Economy Act in their defence in the Newzbin2 case...I wonder if a year from now we will look back and wish we had Sections 17 and 18 instead.[43]

The government’s decision to abandon sections 17 and 18 does not reflect a change of approach to internet censorship. Rather the clear legal precedent established by s97A has given them the opportunity to abandon the troublesome legislation without infuriating the major creative industry corporations who have lobbied so fervently for its introduction. Whether s97A will satisfy their needs is unclear. A legal avenue for blocking websites now exists, but the process of securing an injunction will be slow because it requires court approval. The voluntary scheme touted by Vaizey remains an attractive proposition because it would allow for expedited blocking, and ISPs are likely to be more receptive to cooperating with copyright holders now that it has been established in law that they are responsible for moderating the download activity of their subscribers.

Prevent Strategy

Internet censorship also plays a key role in the government's revamped Prevent strategy, published on 7 June 2011, which aims to tackle terrorism and extremism. It argues that "The internet plays a key role in reinforcing ideology and facilitating activity" and as such "Internet filtering across the public estate is essential. We want to ensure that users in schools, libraries, colleges and Immigration Removal Centres are unable to access unlawful material." The strategy goes further, advocating "...that action is taken to try to remove unlawful and harmful content from the internet." Again due legal process is given short shrift with the scheme touting the idea of ISPs liaising with security services and blocking access to websites on a voluntary basis: "We want to explore the potential for violent and unlawful URL lists to be voluntarily incorporated into independent national blocking lists, including the list operated by the Internet Watch Foundation (IWF)."[44] Ensuring adequate judicial scrutiny of internet censorship seems increasingly to be little more than an afterthought.

The wider context: website blocking in the EU

The UK is not the only country in which internet censorship is currently a hot topic. France leads the way in attempting to police the internet. Since October 2009, a government agency known as HADOPI has enforced a three-strike procedure, similar to the DEA's copyright infringement system, under which individuals who ignore three warnings can have their internet connection suspended for two to twelve months.[45] Official statistics published in July 2011 revealed that 18 million copyright infringers had been tracked in the previous nine months alone, but so far nobody has been cut-off from the internet. Of these 18 million tracked file-sharers, only 470,000 were sent a first warning email, 20,000 a second warning letter, and only 10 were reprimanded for a third time. Their cases are now being reviewed by a judge.[46] These figures imply that warning letters have been a remarkably effective deterrent, but statistics published six months after the introduction of the scheme showed that copyright infringement had actually risen by 3 per cent. The study also showed that roughly half of those who unlawfully file-share also buy legitimate digital content online meaning that, ironically, suspending their internet connections would actually cost copyright holders money.[47]

The system is proving incredibly difficult to enforce, but this has not stopped French President Nicolas Sarkozy from actively promoting greater government regulation of the internet to other EU member

states. In May 2011, he used the E-G8 summit in Paris - an invitation-only gathering of leaders in government and the digital industry - as a platform for his ideas, telling those in attendance that:

The universe you represent is not a parallel universe. Nobody should forget that governments are the only legitimate representatives of the will of the people in our democracies. To forget this is to risk democratic chaos and anarchy.

To this end: "We need to talk to you. We need to understand your expertise, your hopes...and you have to know our limits and our red lines." His approach was met with concern and scepticism by industry representatives in attendance. Google executive chairman Eric Schmidt said: "You want to tread lightly on regulating brand new, innovative industries... I cannot imagine any delegate in this conference would want Internet growth to be significantly slowed by a government that slows it down because of some stupid rule that they put in place." [48]

In Italy, Autorità per le Garanzie nelle Comunicazioni (AGCOM), the regulator and competition authority for the communication industries, agreed in July 2011 to review its plans to pass a resolution giving itself the power to both block and remove material from websites it believes to facilitate copyright infringement. According to European Digital Rights (EDRi), Italy already blocks the widest range of content in Europe. If the resolution is introduced it will operate without any form of judicial oversight.[49]

A draft directive aimed at combating sexual abuse and exploitation of children and child pornography is currently working its way through the EU legislative process. On 12 July 2011, the European Parliament's civil liberties committee emphatically rejected the European Commission's proposal for mandatory blocking of child pornography websites within the EU (by 50 votes to 0, with 3 abstentions). The committee's revised text states that each member state should be allowed to decide whether to do so, and that any blocking must comply with the European Convention on Human Rights, follow transparent procedures and provide adequate legal safeguards.

Incredibly, at a meeting of the Council of the European Union's Law Enforcement Work Party in February 2011, a proposal was made to create a "great firewall of Europe." Under the scheme, "internet service providers would block illicit contents on the basis of the EU blacklist" which would lead to the creation of a "single secure

European cyberspace.” EDRI Advocacy Coordinator Joe McNamee responded: “Most absurd of all, despite all of the costs in terms of democracy, freedom of speech and even the economy, there is no analysis of any benefit or expected benefit that, even mistakenly, the architects of this madness expect to outweigh the cost.”[50] Details of the proposal were published by the Council in May 2011.[51]

Sarkozy’s rhetoric and EU proposals for blanket regulation illustrate just how pivotal a time this is

for internet censorship in Europe. Decisions justified on the basis of combating copyright infringement will adversely affect how all of us access the internet. There is growing recognition of this fact, and a European Commission public consultation published in July 2011 indicated that there is now a clear divide in opinion with copyright holders on one side and ISPs, academics and the general public on the other.[52] As the passage of the DEA illustrates, combating the inordinate amount of influence major corporations exert on European governments and EU institutions will be no easy task.

Footnotes

1 The globe and mail website, 20.5.11:

<http://www.theglobeandmail.com/news/technology/digital-culture/dwayne-winseck/british-report-takes-aim-at-copyright-lobbionomics/article2029680/page2/>

2 <http://www.legislation.gov.uk/ukpga/2010/24/section/17?view=plain>

3 House of Commons Hansard, 3.3.11:

<http://www.publications.parliament.uk/pa/cm201011/cmhansrd/cm110303/debtext/110303-0001.htm>

4 Technical Standard Directive:

http://europa.eu/legislation_summaries/internal_market/single_market_for_goods/technical_harmonisation/l21003_en.htm

5 The Telegraph, 21.3.11:

<http://www.telegraph.co.uk/technology/news/8391308/Digital-Economy-Act-rushed-anti-piracy-laws-delayed-until-2012.html>

6 Slightly right of centre blog, 16.6.11:

<http://www.slightlyrightofcentre.com/2011/06/ofcom-to-spend-estimated-59m-as-real.html>

7 BT press release, 8.7.10:

<http://www.btplc.com/News/Articles/Showarticle.cfm?ArticleID=98284B3F-B538-4A54-A44F-6B496AF1F11F>

8 Treaty on the Functioning of the European Union:

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0047:0200:en:PDF>

9 <http://www.monckton.com/docs/general/BTvBISAPR11.pdf>

10 United Nations Human Rights Council report, p. 21:

http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

11 Organization for Security and Co-operation in Europe report, p. 9:

<http://www.osce.org/fom/80723>

12 Early day motion 1913:

<http://www.parliament.uk/edm/2010-11/1913>

13 The Guardian, 9.5.11:

<http://www.guardian.co.uk/media-tech-law/digital-economy-act-progress>

14 Expert submission to judicial review of DEA, p.6: <http://www.openrightsgroup.org/assets/JK1RC.pdf>

15 London Evening Standard, 2.8.10:

<http://www.thisislondon.co.uk/standard/article-23862448-outdated-wifi-security-leaves-thousands-at-hackers-mercy.do>

16 See: Statewatch journal vol 20 no 2:

<http://database.statewatch.org/article.asp?aid=30000>

17 A quick guide to Norwich Pharmacal orders can be found on the Practical Law Company website:

<http://ld.practicallaw.com/0-211-3137>

18 Open Rights Group submission to judicial review of DEA, p.2: <http://www.openrightsgroup.org/assets/JKillock.pdf>

19 The Guardian, 9.5.11:

<http://www.guardian.co.uk/media-tech-law/digital-economy-act-progress>

20 House of Lords Merits of Statutory Instruments Committee report, p. 2:

<http://www.publications.parliament.uk/pa/ld201011/ldselect/ldmerit/98/98.pdf>

21 Open Rights Group website, 24.3.11:

<http://www.openrightsgroup.org/blog/2011/dea-judicial-review-day-2>

22 British Phonographic Industry website:

<http://www.bpi.co.uk/our-work/policy-and-lobbying/article/second-article.aspx>

23 The Telegraph, 12.4.10:

<http://blogs.telegraph.co.uk/technology/shanerichmond/100004909/steve-lawson-digital-economy-act-makes-me-ashamed-of-musicians-union>

24 Our Kingdom website, 25.3.11:

<http://www.opendemocracy.net/ourkingdom/peter-bradwell/who-decides-what-we-access-on-internet-web-blocking-and-its-dangers>

25 LSE Media Policy Project, 21.3.11:

<http://blogs.lse.ac.uk/mediapolicyproject/2011/03/21/media-policy-project-policy-brief-1-creative-destruction-and-copyright-protection>

26 Open Rights Group website, 10.2.11:

<http://www.openrightsgroup.org/blog/?page=6>

27 House of Lords Merits of Statutory Instruments Committee report, p. 16-17

<http://www.publications.parliament.uk/pa/ld201011/ldselect/ldmerit/98/98.pdf>

28 Authorisation Directive 2002/20/EC:

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0020:EN:NOT>

29 Slightly right of centre blog, 25.1.11:

<http://www.slightlyrightofcentre.com/2011/01/exclusive-ec-raised-concerns-on-uk.html>

30 Open Rights Group submission to judicial review of DEA, p.14-15:

<http://www.openrightsgroup.org/assets/JK1RC.pdf>

31 The Guardian, 25.2.11:

<http://www.guardian.co.uk/technology/2011/feb/25/digital-economy-act-website-blocking>

32 Think broadband website, 5.7.11:

<http://www.thinkbroadband.com/news/4716-ed-vaizey-re-iterates-need-for-site-blocking-system.html>

33 The Register website, 7.7.11:

http://www.theregister.co.uk/2011/07/07/vaizey_at_the_bpi

34 Proposal for voluntary code of practice:

<http://www.openrightsgroup.org/assets/copyrightcensor>

35 Proposal for voluntary code of practice , p. 3:

<http://www.openrightsgroup.org/assets/copyrightcensor/VoluntaryWebBlocking-3.jpg>

36 Tech dirt website, 20.6.11:

<http://www.techdirt.com/articles/20110620/01370314750/universal-music-goes-to-war-against-popular-hip-hop-sites-blogs.shtml>. BitTorrent is a peer to peer programme that allows users to download and upload files, which is not illegal in itself.

- 37 Our Kingdom website, 25.3.11:
<http://www.opendemocracy.net/ourkingdom/peter-bradwell/who-decides-what-we-access-on-internet-web-blocking-and-its-dangers>
- 38 “Site blocking” to reduce online copyright infringement - A review of sections 17 and 18 of the Digital Economy Act:
<http://stakeholders.ofcom.org.uk/binaries/internet/site-blocking.pdf>
- 39 Full text of the judgment:
<http://www.bailii.org/ew/cases/EWHC/Ch/2011/1981.html>
- 40 BBC website, 29.7.11:
<http://www.bbc.co.uk/news/technology-14339223>
- 41 MusicWeek website, 1.8.11:
<http://www.musicweek.com/story.asp?sectioncode=1&storycode=1046130&c=1>
- 42 The Guardian, 29.7.11:
<http://www.guardian.co.uk/commentisfree/libertycentral/2011/jul/29/newzbin2-internet-censorship-bt>
- 43 Open Rights Group magazine, 5.8.11:
<http://zine.openrightsgroup.org/comment/2011/web-blocking-rears-its-ugly-head/>
- 44 Prevent Strategy 2011:
<http://www.homeoffice.gov.uk/publications/counter-terrorism/prevent/prevent-strategy>
- 45 Full title: *Haute Autorité pour la Diffusion des Œuvres et la Protection des Droits sur Internet*, which translates as: *the High Authority for Transmission of Creative Works and Copyright Protection on the Internet*
- 46 The Inquirer website, 14.7.11:
<http://www.theinquirer.net/inquirer/news/2094142/france-contacts-470-million-tracked-filesharers>
- 47 Torrent Freak website, 9.3.10:
<http://torrentfreak.com/piracy-rises-in-france-despite-three-strikes-law-100609>
- 48 Huffpost Tech website, 27.5.11:
http://www.huffingtonpost.com/don-tapscott/we-need-more-internet-not_b_868162.html
- 49 EDRi website, 13.7.11:
<http://www.edri.org/edriagram/number9.14/internet-blocking-agcom-italy>
- 50 EDRi website, 4.5.11:
<http://www.edri.org/edriagram/number9.9/virtual-schengen-border>
- 51 EDRi website, 12.5.11:
http://www.edri.org/virtual_schengen
- 52 Torrent Freak website, 11.7.11:
<http://torrentfreak.com/isps-academics-and-citizens-oppose-eu-anti-piracy-legislation-110711>

© *Statewatch* ISSN 1756-851X. Personal usage as private individuals/"fair dealing" is allowed. We also welcome links to material on our site. Usage by those working for organisations is allowed only if the organisation holds an appropriate licence from the relevant reprographic rights organisation (eg: Copyright Licensing Agency in the UK) with such usage being subject to the terms and conditions of that licence and to local copyright law.