Online Copyright Infringement Provisions within UK's Digital Economy Act, 2010 - Are Internet Service Providers Legally Responsible for their Subscribers?

Author: Eben Duah

Abstract

In recent years, there have been legislative developments internationally, encouraging internet service providers (ISPs) to co-operate with rights holders in tackling the problem of file-sharing. This framework has been brought sharply into focus by the increasing use of the internet to share copyrighted materials without rights holders' permission or authorization. The UK's Digital Economy Act, (DEA) which became law in 2010, contains provisions that place legal obligations upon ISPs to co-operate with rights holders in achieving this set goal. Under the terms of the statute, ISPs will be obliged to notify subscribers whose accounts are suspected of being involved in copyright violating activities; to supply infringement lists to rights holders upon request for the purpose of legal actions, and also to employ technical measures including the traffic management of persistent infringers' internet access and the blocking of infringing sites. This legislation has however invited criticisms, not least from the ISPs, who share a growing concern that the obligations imposed by the Act may not be well-suited with EU laws design to ensure that national laws are proportionate. It is also asserted that any legal obligation enforced upon the ISPs to 'police' the internet would also raise data protection and user privacy issues. This paper therefore attempts to examine the extent to which the Act conflicts with important European rules and assess ISPs liability for users' behaviour.

Introduction

Since the launch of the peer-to-peer (P2P) programmes in the late 1990s, file-sharing has featured prominently in online copyright infringement debates. There have been strategies to try to reduce such unlawful activities which have encompassed legal actions against P2P vendors and individual infringers, while internet service providers' (ISPs) have also been requested to comply with procedures such as notice and take-down and install filtering systems. Although, the legal actions have resulted in shutting down most of the mainstream P2P networks including *Napster[2001]* and *Grokster [2005]*, and court requests seeking to get users' identities from ISPs have largely been granted through disclosure orders, (or Norwich Pharmacal orders) there are still problems with these strategies. For example, the decentralised architecture of the P2P networks has made it difficult for right holders to pinpoint where to level blame, individuals have increasingly been resorting to the use of

pseudonyms or virtual private networks to evade or complicate detection, and particularly the cost ineffectiveness of legally pursuing the millions of illegal file-sharers with the low risk of prosecution appears to have led to a rethink and thoughts of a new focus.

ISPs in the Picture

In an effort to find an alternative solution, there have been calls for ISPs to take a more active role in 'policing' their networks by being part of a technical enforcement regime, popularly referred to as the "graduated response" or "three strikes" approach. The graduated response model (GRM) proposes to begin with the gathering of evidence through the harvesting of alleged infringers' internet protocol (IP) addresses. It also involves the notification of alleged infringement and internet traffic management which the International Federation for the Phonographic Industry (IFPI), in particular has been demanding governments to require ISPs to enter into cooperative relationship with right holders in order to fight illegal file-sharing. Global reception to this model have been, and as to be expected, mixed. Although, some countries such as South Korea and Taiwan have already incorporated the GRM into their domestic copyright enforcement systems, (De Beer and Clemmer, 2009) and the United States (Anderson, 2008) and Ireland (Anderson, 2009a) have agreed to voluntary schemes, Germany and Finland have so far refrained from, or rejected the GRM implementation, - just to name but a few. (Cheng, 2009; Llewellyn, 2009; Moya, 2010) Within Europe, there have been two major developments regarding GRM legislation. France adopted a so-called HADOPI law in 2009, (*HADOPI in English: "Higher Authority for the Diffusion of Works and the Protection of Copyright on the Internet"*) while the UK's Digital Economy Act (DEA) passed into law in 2010 also has provisions to essentially impose a GRM obligation on ISPs. Before discussing the DEA provisions and the ISP obligations which form the core of this paper, it is vital to provide a brief background to the HADOPI law which appears to be a pioneered GRM legislation.

The French HADOPI

In 2006, the French adopted the DADVSI law, (*in English: "law on authors' rights and related rights in the information society"*) which implemented Directive 2001/29/EC. The DADVSI had provisions [Article L.335-12 of the Intellectual Property Code] that obliged subscribers to monitor their accounts to ensure that no file-sharing occurred. The DADVSI however faced challenges including the practicalities of prohibiting all P2P transferring activities, while it was also believed to restrict the right to copying copyrighted works for private use due to its text on the digital rights management. The French Constitutional Counsel then struck down several of its major provisions based on its unconstitutionality, *[Decision no. 2006-540 DC, 27 July 2006]* thereby making the DADVSI much weaker in terms of fighting online copyright infringement.

However, that did not frustrate the French pursuit for online copyright infringement legislation and France eventually became the first EU Member State to put into effect GRM legislation as a way of enforcing copyright on the internet by sanctioning users. It began with the construction of the *HADOPI-1* (Bill), described as more suitable and efficient measure than the DADVSI provisions to fight illegal file-sharing. (May and Liens, 2009) The key goals of this bill were the setting up of an administrative authority called HADOPI, to oversee the implementation of a GRM regime which would include the suspension of internet access alongside the education and promotion of legal online alternatives without the involvement of any judicial authority. Nonetheless, the French Constitutional court called for

amendment to parts of the bill, [*Decision no. 2009-580 DC, 10 June 2009*] citing some of the texts as in breach of an individual's freedom of expression under the Constitution. The Counsel, utilising its powers under Article 61(2) of the French Constitution (1958) also observed illegitimacy on the judicial role of the administrative authority with no recourse to the courts. Besides, there were concerns as to whether due-processes had been adhered to, in areas such as fair trial, the presumption of innocence and the right to defence. (Lucchi, 2011) These concerns were to be addressed with a revised *HADOPI-2* to overcome constitutional challenges, so as to pave the way for the enactment of the so-called HADOPI law in 2009. It must be pointed out that the adoption of HADOPI-2 has also been challenged, but rather unsuccessfully, as opponents still believe it raises, amongst other things, issues of privacy to which internet subscribers are entitled. With the HADOPI law now passed, its implementation process involves detection by the copyright owners of potential infringements (based on IP addresses) over P2P networks to be reported to the HADOPI administrative authority. The HADOPI authority then consults with other parties involved, and if contented, contact the relevant ISPs to seek the identification of these alleged infringers, (May and Liens, 2009) while also requiring the ISP to send the first notification to the matched subscriber. (Lovejoy, 2011) A second notice is sent, if the IP address of the subscriber first notified is suspected of being engaged in another infringement over the subsequent six months. (Lovejoy, 2011) If within one year after the second notice, a user's IP address again appears among those reported to the HADOPI authority, the user will then be subjected to judicial procedures to determine guilt, where penalties ranging from fines through to the disconnection of an internet could be expected, but with the option of subscribers appealing the judge's decision. (Stroussi, 2009) Some commentators argue that this procedure is disproportionate on the basis that a referral of repeat offenders to a judge may result in nothing more than the judge overseeing a penalty being imposed without oral hearing from the alleged infringer in defence of the allegation. With minimal participation of the parties to determine guilt, it gives the impression of a set-up akin to an administrative body with a legal representative just "presiding over" decisions. (Stroussi, 2009) Does this procedure not challenge the 'presumption of innocence' principle? [*Article 9 of the Declaration of the Rights of Man and of the Citizen of 1789*]

Other concerns also point towards whether or not subscribers' access to other IP based services would be unaffected in the event of an internet suspension. According to Horten, (2009) there may be the difficulties in applying internet suspension across France without affecting some account holders' other subscriptions within a package. (Horten, 2009) Horten's findings appear to be based on a reference to an assessment by the French regulator (ARCEP) which indicates that in areas where there is no local loop unbundling, it will be impossible to maintain IP-based voice services, when terminating internet access. If this occurs, the "disproportionate" arguments will be strengthened. However, despite the criticisms, doubts of unconstitutionality and unprecedented debates surrounding HADOPI-2, its implementation by the French government has seen suspected copyright infringers receiving warning letters since September, 2010. (Forde, 2010) Let us now focus on the UK legislation, the Digital Economy Act 2010.

The Digital Economy Act, (DEA) 2010

The UK became the next European Union (EU) Member State, after France, to legislate on the GRM by passing the DEA in 2010. The enactment of the DEA has been the culmination of proposals and consultations following recommendations from the Gowers Report in 2006 and then the Digital Britain report (DBR) in 2009 when the digital inclusion targets were set

and the objective of reducing illegal file-sharing by encouraging cooperation between ISPs and rights holders was outlined. (Carter, 2009) This was followed by the Digital Economy Bill in the same year which adopted a number of proposals set out in the DBR. With the passing of the DEA, the United Kingdom's (UK) communications regulator (OFCOM) has been responsible for the specification, procedural and enforcement elements of the obligations through the approval or adoption of legal binding codes of practices. Before the examination of the contested DEA provisions, a background to the status and origin of the obligations code are set out below.

Initial Obligations

Driven in part by the fact that existing strategies are not working, the DEA 2010, through its amendment to the Communications Act 2003 (CA 2003), imposes specific initial obligations on the ISPs, within sections 124A CA 2003 and 124B CA 2003, with the prescribed content of the initial obligations in 124E CA 2003. A GRM within the DEA commences with the supply of a copyright infringement report (CIR) by the rights holder to the appropriate ISPs (usually within a month of the alleged detection of the infringement) including details of the subscriber's internet protocol (IP) address and evidence of the infringement and the time of occurrence. The ISP is then required, also within one month of the receipt of the CIR, [and pursuant to 124A (4)], to notify the subscriber of the alleged offence, [as set out within 124A (6)] while also designing and maintaining a copyright infringement list (CIL). ISPs must also suggest alternative legal channels for copyrighted material consumption and convey any other advice, deemed helpful to the alleged infringer. [124A (8)] Section 124B CA 2003 then imposes upon ISPs an obligation to provide copyright infringement list (CIL) in a non-identifying format to copyright owners upon request, or as the initial obligations code requires the ISPs to comply, for rights holders to be able to secure a court order to then learn of the identity of the serial offender for possible legal action. The initial confusion from this information exchange may raise the question why the copyright owners would somehow be able to write a CIR for the ISPs then require a set list from the ISPs based on the CIRs. The clearest assumptions may be that, the copyright owners have no way of identifying any alleged infringer, simply by the IP addresses alone and since ISPs would normally not disclose the identity without a court order due to the confidentiality agreements they have with their subscribers, the information that passes 'to-and-fro' (as the code may dictate) eventually enables right holders to obtain a disclosure order. Furthermore, some of the subscribers are assigned new (dynamic) IP addresses each time they are connected to the internet, hence, the information provided in the CIL will ensure a match of any particular infringement with the specific account holder.

Technical Obligations

While there was the initial fear of an imminent termination of subscriber's internet access after the warnings, such as within the HADOPI law, there is no such imminence in the DEA. Rather, an assessment based upon the sufficiency of the initial obligations alone to contain file-sharing will be made by OFCOM to determine whether a technical obligation should be imposed on ISPs. This means that any anticipated technical measures will only be considered if the implementation of an initial obligations code has failed to reduce online copyright infringement by about 70 percent. (Harding, 2010) Following an assessment and preparation procedure, pursuant to 124G CA 2003, it will then allow for the Secretary of State to impose an obligation on ISPs to implement technical measures. [124H] The technical measures, as defined in 124G(2), are expected to be taken against some or all "relevant subscribers"

(124B(3)) for the purpose of preventing or reducing infringement of copyright by means of the internet. These will include; limiting the speed or other internet capacity of the service provided to a subscriber; preventing a subscriber from using the service to gain access to particular material; suspension of service provided to a subscriber or; limiting the service provided to a subscriber in any other way. [As in 124G(3)] Section 124J, then sets out contents of code about obligations to limit internet access and so the three sections [124G, 124H, and 124J] read together therefore strengthen the Secretary of State's powers to impose technical measures on the ISPs. At this point the "suspension of services provided to a subscriber" if introduced arguably makes it on a par with HADOPI.

Furthermore, the Secretary of State may by regulation also make a provision about the granting by 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 conjunction with an activity that infringes copyright under section, 17(1), DEA. This proposed regulation then states that, an injunction may not be granted unless satisfied that it abides by the content set out within 17(4) and 17(5) DEA. The test of "is being or is likely to be used" within section 17(1) may be broad, given that section 17(4), provides an extension of an injunction to apply not only to content hosting sites, but also to access facilitators. While this may sit in well with the goal of prohibiting access to specific file-sharing linking sites, such as BitTorrent sites, the section contains vague interpretation of the types of website that the provision is restricted to, leading to the possibility of non-infringing sites also being subjected to injunction within the meaning of section 17 DEA, should the need arise. This route, if pursued, will no doubt also represent a proportionality problem.

The Tension in ISP Obligation

It has been noted that especially since 2007, the growing encouragement of the GRM has been at the forefront of the international lobbying campaign being waged by digital right holders to address illegal file-sharing. It does also suggest an attempt to legalise the right to monitor, while also affirming the principles that copyright should be respected and infringement punished. (Rayna and Barbier, 2010) Right holders may have hoped for routine monitoring of infringing activities by ISPs as an integral part of service without the need for right holders' intervention or possibly a judicial system, (Edwards, 2008) and if that could have been achieved, it would potentially reduce the costs of pursuing file-sharers. (Rayna and Barbier, 2010) However, and also as expected, this "GRM crusade" has brought tensions between digital right holders and ISPs on various fronts, not least an uneasy relationship between ISP immunities and copyright law enforcement which then begs the question as to whether or not, ISPs should be "responsible for the actions of their subscribers". (Baskerville & Baskerville, 2010, pp; 496)

ISPs have been made responsible for their users' behaviour especially with issues relating to criminal activities, but have been somewhat reluctant, possibly backed by the immunities under the ECD, to comply on civil related activities in the course of their service provision except upon knowledge and/or complicity. Although, determining the "knowledge or complicity" element and how impartial or credible such evidence might be, (given that they are often produced by the copyright holders or their affiliates) is debatable. Let us now move the discussion onto assessing the scope of ISP obligation in relation to immunities under the ECD.

Scope of ISP Obligation

Since the ISP's role is to act as gatekeepers to the internet, they have also been exposed to increased risks in content liability hence, the search for, and the granting of immunities from liability enshrined within the ECD [Directive 2000/31/EC]. The ECD provisions therefore create a regime of defences to ISPs who transmit copyright materials and occur when an ISP establishes that they are just mere conduits, (under Article 12) are merely caching information (Article 13) or hosting information (Article 14) provided they comply with specified statutory conditions. These may be where it is established that ISPs are not involved in selecting or initiating such transmissions (Article 12(1) a-c) and act expeditiously to take down or disable access to such information upon knowledge. (Articles 13 (1e) and 14 (1b)) An example of an ISP being exempted from infringement liabilities can be found in a recent decision in *Roadshow Films v iiNet, 2010 [FCA 24]* where an Australian court ruled that iiNet (An ISP) cannot be held liable for its customers' illegal movie downloading by means of the BitTorrent P2P system. This was based on the Court's findings that the ISP had not authorised any infringements and had also complied with adequate procedures to qualify for such immunities. Although, Australian judgments are not binding in the UK courts and this ruling is more one of assessing an ISP liability for authorising infringement *[CBS v Amstrad, 1988]* rather than enforcement, it perhaps set out the extent to which an ISP safe harbour based on subscribers' infringing activities could be determined. In any case, the liability exemption provided under the ECD will not affect the possibility that a court or administrative authority, in accordance with Member States' legal systems could require the service provider to terminate or prevent an infringement. (Articles 12(3), 13(2) and 14(3)) In terms of any monitoring obligations, ISPs have sought refuge in Article 15(1) of the ECD in particular when such obligations may be imposed upon them. This provision specifically states that;

> "Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity".

Factoring this into the requirement imposed upon ISPs by sections 124A and 124B CA 2003 there has been the suggestion that this obligation potentially infringe Article 15(1) thus, if a general obligation to monitor could be established. Nonetheless, whether or not the obligation imposed upon ISPs by the DEA contested provisions amounts to monitoring has been raised in *BT Plc & Anor. v The Secretary of State [2011] EWHC 1021*, which will be examined at the end of the paper.

It is also worth pointing out that, in the event of a general obligation on ISPs to monitor being established by the DEA, there may be other compounding challenges on its enforceability given that the UK implementation of the ECD omits the terms set out in Article 15(1) and does not seem to replace them with any similar prohibition. Possible conflicts will include whether or not the UK is fully in compliance with the applicable EU law and whether the *EMI v UPC, [2010 E.C.D.R. 17]* test would or might apply. This was an Irish case where an injunction could not be granted because an appropriate legal basis was not available under national law. While ISPs are to enjoy immunities under the ECD, copyright owners are also provided with the legal means by which to enforce their rights largely through court orders.

Copyright Holders' Rights

ISPs appear to have long been immune from any such enforcement until the encouragement of the GRM, which in practical terms, see ISPs as better placed to observe and/or record

users' behaviour. This notion is also emphasised by Recital 59 of Copyright Directive, 2001/29/EC, which states that;

> "In the digital environment, in particular, the services of intermediaries may increasingly be used by third parties for infringing activities. In many cases, such intermediaries are best placed to bring such activities to an end ... This possibility should be available even where the acts carried out by intermediary are exempted under Article 5. The conditions and modalities relating to such injunctions should be left to the national law of the Member State."

The usual channel to achieve ISPs' disclosure of personal information has been through the Norwich Pharmacal order, following the ruling in *Norwich Pharmacal Co v Customs & Excise, 1974.* [*1974 AC. 133*] This line of authority allows information to be obtained from third parties which may enable the identification of wrongdoers and trace the proceeds of wrongdoing and right holders have had little problems with being granted court orders to obtain the personal data from ISPs. *[Polydor v Brown, 2005, EWHC 3191 (Ch)]* In the recently contested "volume litigation" in the UK, this route was heavily pursued (Murray, 2010) which also resulted in false positives. [*Media CAT Ltd v Adams & Ors [2011] EWPCC 6, para, 34]* Besides, the UK E-Commerce (EC Directive) Regulations, 2002 sets out right holders' right to apply to a court for relief so as to be able to prevent infringement of rights, (see; Regulation 20) while, aspects of Article 15,(ECD) also appear to weigh in favour of the DEA obligations. Under Article 15(2);

> "Member States may establish obligations for information society service providers to promptly inform the competent public authority of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities at their request, information enabling the identification of recipients of their service with whom they have storage agreements"

What may complicate this right would be whether or not right holders who seek information such as the CILs from the ISPs fit the description of a competent public authority rather than a private entity. Another right enforcement provision can be found within Article 8(d) of the IP Enforcement Directive - IPRED [Directive 2004/48/EC] which require Member States to ensure that in the context of proceedings concerning the infringement of IP rights and in response to justified and proportionate request from claimants (right holders) the competent judicial authorities may order the provision of information on the origin and distribution networks of (goods and) services which infringe IP rights. Then, Article 8(3) of the EU Copyright Directive - EUCD (Directive 2001/29/EC) also sets forth the requirement of Member States to ensure that rights holders are in the position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right. By the definition of an intermediary to cover P2P networks as well as an ISP, it therefore gives meaning to the contested injunction provisions under section 17 of the DEA.

Some EU Developments on ISP Monitoring and Data Disclosure

In what was hailed as the first European court to rule on an ISP compliance with filtering orders, the Court of First Instance in Belgium in 2007 ordered the ISP (Scarlet) to block or filter out traffic on its network. [*SABAM v SA Scarlet. [2007] E.C.D.R. 19*] This case had been brought by the Belgian authors' rights group SABAM, who believed the order was necessary to prevent infringement of its members' copyright. Although, it has been controversial from the start of the proceedings and the ruling by the Court of First Instance was believed to have impacted on the scope of ISP obligation, it could still be possible due to the diverse interpretation of implemented EU laws at national levels. Whether or not the

EUCD or the IPRED superseded the ECD, the court had maintained that although the mere conduit defence was not relevant to the case, the duty imposed on the ISP still protected the mere conduit exception and that its injunction also prohibited a general obligation to monitor the network. It was to be followed by a Danish court ruling also permitting filtering, [*SONOFON A/S v IFPI Denmark [2009] E. C. D. R. 10]* based on its interpretation of a transposed EU law. Following on from SABAM [2007] ruling, the ISP Scarlet pursued an appeal against the verdict and successfully won a court reprieve prompting the national court to now refer questions to the ECJ. *[C-70/10 SABAM Extended v Scarlet]* The guidance sought by the referral is for the ECJ to rule on whether a national court can order an ISP to install a system for filtering and blocking electronic communications in order to protect IP rights.

A recent ECJ development in the SABAM case *[C-70/10 SABAM Extended v Scarlet]* has been the Advocate General's opinion which considers that Scarlet should not have to filter copyright-infringing traffic from its service as to do so would be a restriction on the right to respect for the privacy of communications and the right to protection of personal data, both of which are rights protected under the Charter of Fundamental Rights. This reinforces the view that whereas IP is a property right, data protection being related to privacy is more akin to a human right. And by the same token, (according to the opinion) the deployment of such a system would restrict freedom of information, which is also protected by the Charter of Fundamental Rights. (ECJ Press Release, 2011) The implication of the Advocate General opinion (if followed in the judgement) will complicate efforts by right holders to secure "rubber-stamped" monitoring obligation by ISPs through court orders. Furthermore, this opinion, if followed, would also suggest the importance of, at least, enabling the ECD and EUCD to complement each other rather than the EUCD superseding the ECD as was largely thought to have been the issue in the SABAM 2007 ruling.

In relation to personal data disclosure, the ECJ judgments in the *Tele2, [2009]* and *Promusicae [2008]* cases provided some neutral interpretations. Although these decisions appeared vague and left the balancing exercise to be completed by the national courts, they have stressed the need to balance both copyright and the rights of consumers through the application of national laws by Member States. In the Tele2 case, [*C-557/07) LSG v Tele2*] it was held that the Community provisions (Article 8(3) of Directive 2004/48/EC and Article 15(1) of Directive 2002/58/EC) do not preclude Member States from imposing an obligation to disclose third parties' personal data to enable civil proceedings for copyright infringements. It then stated the need for any applicable law being transposed into national laws, to comply with the balancing of the fundamental rights involved while also considering the general principles of Community law such as the principle of proportionality. The ECJ in *Promusicae,* [*C-275/06 Promusicae v Telefonica*] was also confronted with the consideration of the application of a number of directives and separate provisions to provide clarity on the balancing of rights. Here, the ECJ recognised that any obligation to disclose personal data had to be in order to ensure the effective protection of copyright in the context of civil proceedings. The Court also recognised that any obligation to disclose confidential personal data must then respect Articles 7 and 8 of the Charter of Fundamental Rights that require protection for the right to respect for family and private life and the right to the protection of personal data. The ECJ then held that when implementing such directives, laws must be interpreted by national courts and authorities in a manner consistent with the directives but not to rely on an interpretation which conflicts with these rights as well as considering the principle of proportionality.

It could be deduced from the outcome of both cases [*Tele2* and *Promusicae*] that as long as the general principle of proportionality and the balancing of rights can be considered at the national level, the disclosure of personal data in civil cases to enforce property rights is at least permissible. This may then justify efforts by the right holders to actively engage in identity disclosure procedures in response to copyright infringement within the meaning of the DEA obligations, although users' privacy and data protection concerns have also emerged. Furthermore, the reliance on national laws with its vast number of optional exceptions within implemented directives then means Member States can pick and choose at will, which consequentially also impact on efforts at EU harmonisation of rights. Before moving on to the evaluation of relationships between ISPs and right holders and possible implications from recent developments on ISP obligations, some aspects of proportionality needs to be highlighted in the context of the DEA provisions.

The Proportionality Debate

In assessing proportionality, several issues may be considered. This may include whether or not the DEA contested provisions are set out to specifically achieve the goal of reducing illegal file-sharing or exceed its mandate, whether they are necessary and appropriate, or how far it encroaches on consumer rights. More importantly, the impact of a technical measure where subscribers (or innocents sharing the same account) could be deprived of their internet access continues to form a major part of the proportionality debate and violation of subscribers' fundamental rights.

Such uneasiness, among other things, prompted a recent judicial review of the DEA by the UK High Court, demanded by two of UKs biggest ISPs (BT and TalkTalk) who wanted clarity and certainty on the law before its implementation. The High Court then agreed to review the law to see whether the DEA conflicted with EU laws on privacy and ISPs' liabilities for users' behaviour. (Ashton, 2010) At the hearing, five grounds of challenge were advanced by the Claimants in respect of the contested provisions which related to the EU's Technical Standards Directive, (TSD) the Authorisation Directive, (AD) the E-Commerce Directive, the Privacy and Electronic Communications Directive and on the proportionality principle. In the Court's judgement, all but one of the challenges advanced were dismissed, indicating that the directives had not been breached and at least the DEA, as it stands, is proportionate. *[BT Plc & Anor. v The Secretary of State [2011] EWHC 1021]* Although in the context of this paper, aspects of TSD and AD are not discussed. In terms of the necessity of the DEA provisions, arguably copyright needs to be protected hence various provisions within national and EU laws to order ISP compliance with IP enforcement online. The mere-conduit provision (Article 12 ECD) being one of ISP defences could be interpreted as striking a careful balance between the different interests involved, given that ISPs are free to provide services to their subscribers but then to also cooperate with copyright enforcement when prompted to do so. *[BT Plc & Anor. v The Secretary of State [2011] EWHC 1021]*

Another area of concern by the interveners related to why an existing line of authority such as a Norwich Pharmacal line of authority is not used as perhaps a less restrictive option. This preference therefore also required a comparison to be made between this order and the DEA obligations. Assuming that the Norwich Pharmacal order is less restrictive, it could also be more intimidating in that, once a subscriber's identity has been disclosed by the ISP, the usual form of contact with the alleged infringer is a so-called "speculative invoice" seeking immediate financial compensation for which in the case of default, court proceedings are the only alternative. This may not be the same with the DEA where, the processes set out in the

obligations code begins with a notification[s] alongside education to assist the alleged subscriber to desist, secure subscription account and opt for a legal alternative. While a technical obligation within the DEA will only be considered and scrutinised before its introduction or may never be introduced if the initial obligation alone accomplishes the set goal. The classical proportionality question then will be whether or not even a less restrictive measure achieves the same objective?

The judicial review judgement had also sought to justify the lengthy consultation processes which took into account representations by all stakeholders to have resulted in a balance being struck with all interested parties before its enactment hence, proportionality considered. *[BT Plc & Anor. v The Secretary of State [2011] EWHC 1021, para, 212]* Although, there could be a potential risk of a "chilling" effect arising from the introduction of a technical measure, since the measures are not even operational and hence no accumulation of experience of their effects in practice, it would be premature to conclude the impact of any chilling effect from a measure that is yet to be implemented. *[BT Plc & Anor. v The Secretary of State [2011] EWHC 1021, para, 240]* In any case, if a technical measure will be introduced to include the termination of internet access, it is bound to clash with aspects of users' human rights as recently reported. (La Rue, 2011)

The Judicial Review Judgement – Any Clarity?

In order to measure whether or not the recent judicial review judgement provides any clarity on the ISP obligations, we would perhaps be reminded that, while general monitoring of subscribers conflict with the earlier measures, (see; Article 15(1) ECD) specific monitoring seems to be supported and emphasised by Recital 47 of the Directive. It states that while;

> "Member States are prevented from imposing a monitoring obligation on service providers only with respect to obligations of a general nature; this does not concern monitoring obligations in a specific case and, in particular, does not affect orders by national authorities in accordance with national legislation".

This then shift the focus onto what kind of obligation the DEA provisions propose, pursuant to 124A and 124B CA 2003. It could be assumed that the initial obligations does suggest nothing more than a specific obligation between ISPs and other parties. Whether or not such obligations can be regarded as monitoring has required urgent clarification and which seems to have been given in *BT Plc & Anor. v The Secretary of State [2011] EWHC 1021*. The judgement found that the DEA imposed no general obligation on the UK participating ISPs to monitor any information, nor a general obligation to actively seek facts or circumstances indicating illegal activity. (Article 15(1) ECD)

The Court sought to clarify that the CIR data to be handled by the ISPs (under 124A CA, 2003) will be nothing more than merely reporting to the subscriber, information received from the right holders of alleged infringement. While the maintenance of the CILs by ISPs, (124B CA, 2003) will also amount to a mere compilation of CIRs in respect of a repeat infringer, rather than an obligation to monitor that information. The Court, emphasising no breach of Article 15(1) ECD also pointed out that, right holders have been the parties who actively seek facts and circumstances indicating illegal activity through the harvesting of IP addresses of alleged infringers, as prescribed by the DEA. In other words, it is the copyright owner, rather than the ISP who conducts the (monitoring) investigation and the CIR becomes a work product of another party, while the CIL is simply a compilation of such reports in respect of the relevant subscriber. [*See; BT Plc & Anor v Secretary of State [2011] EWHC*

1021, para 116-118] Now, how do the recent developments in both the DEA review and the consideration of the SABAM case by the ECJ impact or affect ISPs responsibilities for users‟ behaviour?

Possible Implications and Directions?

Based on the judgement in, *BT Plc & Anor v Secretary of State [2011] EWHC 1021,* and assuming that an appeal which is now being sought by Claimants (BT Press Release, 2011) does not alter this ruling, an interesting interpretation would have emerged about the responsibility of ISPs under a GRM. The ruling as it stands establishes that the DEA imposes no general obligation on ISPs to monitor hence especially the ECD is not breached and the DEA is lawful. On the other hand, if the recent Advocate General's opinion in *SABAM [C-70/10]* is followed in the ECJ judgement, it may be that the installation of systems (at issue) by the ISP Scarlet, would potentially filter all data communications passing via Scarlet's network in order to detect copyright infringing data which in the Advocate General opinion, will constitute a general obligation to monitor and hence will be in breach of the fundamental rights of subscribers (ECJ Press Release, 2011)

In summing up the implications and possible direction of the responsibilities imposed on ISPs vis à vis their subscribers, there is the indication that a GRM such as the one legislated by the DEA, (involving third parties tasked with investigating infringement) may not hinder ISP obligations to comply and cooperate with right holders and in fact be legal. Whereas, if the court imposes a direct order on ISPs to install monitoring systems to filter and block content, (absent other investigating parties) a general obligation to monitor may be established which would potentially be in breach of subscribers' fundamental rights and therefore unenforceable, as the Advocate General has suggested. Importantly, it is worth mentioning that these developments may still not hinder a national court's power to impose more specific obligations on intermediaries, and it is hoped that the ECJ judgement in SABAM *[C-70/10 SABAM Extended v Scarlet]* will eventually help clarify aspects of ISP obligations in addressing copyright infringements.

Conclusion

In assessing the goals of the DEA online copyright infringement provisions, it is becoming increasingly essential for right holders to require access to a trail of evidential materials kept by the ISP, when internet is accessed so as to enable the enforcement of their rights and especially when fighting illegal file-sharing. These efforts, despite successes through the use of Norwich Pharmacal orders and currently with the GRM, has also kept the users' confidentiality and right to privacy debates alive requiring clarity on the balancing of rights as well as the need for rules on copyright and e-commerce to complement each other. On the principle of proportionality, it appears that, a vivid assessment of its impact in relation to the DEA may still be contingent on the Code taking legal effect as the initial obligation may or may not trigger a technical obligation. While, ISPs sit in between subscribers and copyright enforcers, there appears to be a very difficult task to accomplish, not least, having to deal with the somewhat uneasy relationship between the immunities under the ECD and the responsibilities under copyright law. Also, as the internet arguably shifts from being a luxury into a right, governments are faced with the complicated task of achieving an ostensibly impossible middle-ground in satisfying both the copyright holder and consumers. Perhaps there is the need for any copyright enforcement to take into account the importance of ISP immunities and fundamental values of the end-users when achieving such goals given that the

ISP's primary responsibility is to provide a transit service to its subscribers by its role as a gatekeeper to the internet.

References and Bibliography

Books

Baskerville, D. & Baskerville, T. (2010 pp; 496) The Music Business Handbook and Career Guide. 9th Edition. Sage Publication. California.

Casey, T (2001) ISP Liability: Survival Guide, Strategies for Managing Copyright, Spam, Cache and Privacy Regulations. John Wiley & Sons. USA

Edwards, L and Waelde, C (2009) Law and the Internet. Hart Publishing. Oxford, UK.

Lim, Y. (2007) Cyber law: Commentaries and Materials. 2nd Edition. Oxford University Press. Melbourne.

Cases

A&M Records Inc v. Napster, Inc 239 F.3d 1004 (9th Cir. 2001)

Ashdown v Telegraph Group Ltd, [2001] EWCA Civ 1142

Bonnier Amigo Music Norway AS v Telenor Telecom Solutions AS [2010] E.C.D.R. 2

British Telecommunications Plc & Anor. R (on the application of) v The Secretary of State for Business, Innovation and Skills [2011] EWHC 1021(Admin)

Case – C-275/06 Productores de Musica Espana v Telefonica [2008] 2 C.M.L.R. 17

Case – C-557/07 LSG Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v Tele2 Telecommunication GmbH [2009] OJC 113/14

Case – C-70/10 Scarlet Extended SA v SABAM OJ [2010] C 113/30

CBS Songs Limited v Amstrad Consumer Electronics Plc [1988] 2 WLR 1191

Durant v FSA, [2003] EWCA Civ. 1746, Court of Appeal (Civil Division)

EMI (Ireland) Ltd v Eircom Ltd [2009] IEHC 411 (HC Irl)

EMI (Ireland) Ltd v Eircom Ltd [2010] IEHC 108 (HC Irl)

EMI Records (Ireland) and Others v UPC Communications Ireland Ltd [2010] E.C.D.R. 17

Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259 (9th Cir. 1996)

Media CAT Ltd v Adams & Ors [2011] EWPCC 6

Metro-Goldwyn-Mayer Studios v Grokster Ltd, 125 S. Ct. 2764 (2005)

Norwich Pharmacal Co v Customs & Excise, [1974] AC. 133

Polydor Limited and Others v Brown and Others, [2005] EWHC 3191 (Ch)

Roadshow Films Pty Ltd v. iiNet Limited, [2010] FCA, 24

SABAM (Societe Belge des Auteurs, Compositeurs et Editeurs) v SA Scarlet. [2007] E.C.D.R. 19

Shapiro, Bernstein and Co. v. H.L. Green Co., 316 F.2d 304 (2d Cir. 1963)

SONOFON A/S (formally DMT2 A/S) v IFPI Denmark [2009] E. C. D. R. 10

Totalise PLC v Motley Fool LtD & Another, [2001] EWCA Civ 1897

Twentieth Century Fox Film Corporation v Newzbin Ltd [2010] EWHC 608 (Ch)

Legislation/Directives/Conventions

Authorisation Directive (Directive (2002/20/EC)

Charter of Fundamental Rights of the European Union, [2010/c 83/02]

Digital Millennium Copyright Act (DMCA)

Electronic Commerce Directive (Directive 2000/31/EC)

Privacy and Electronic Communications Directive (Directive 2002/58/EC)

The Copyright, Designs and Patents Act (CDPA) 1988 (c. 48)

The Data Protection Act, 1998

The Data Protection Directive (Directive 95/46/EC)

The Digital Economy Act, (2010) Chapter 24

The Electronic Commerce (EC Directive) Regulations 2002, [SI 2002/2013]

Journals

De Beer, J. and Clemmer, C. (2009) Global Trends in Online Copyright Enforcement: A Non-Neutral Role for Network Intermediaries? Jurimetrics Journal, 49, 375–409.

Harding, T. (2010) The Digital Economy Act, 2010: Content and Implications. Journal of E-Commerce Law and Policy, 12 (5), 3-5.

Lambrick, J. (2009) Piracy, File Sharing … And Legal Fig Leaves. Journal of International Commercial Law and Technology, 4(3), 185-195.

Ucchi, N. (2011) Cardozo Journal of International and Comparative Law (JICL), Vol. 19, 2011, pp; 1-28.

Luck, M. (2009) Internet Policing and Regulation. Journal of E-Commerce Law and Policy, 11 (6), 3.

May, B. and Liens, M. (2009) France's Attempt to Introduce Anti-Piracy Legislation. Journal of E-Commerce Law and Policy, 11 (7), 10-12.

Philips, J. (2009) Three Strikes' . . . and Then? Journal of Intellectual Property Law & Practice, 4(8), 521.

Rayna, T. & Barbier, L (2010) Fighting Consumer Piracy with "graduated response": An Evaluation of the French and British Implementations. International Journal of Foresight and Innovation Policy, 6(4), 294-314.

Weston, M. (2010) DEA 2010: Wi-Fi Liability. Society for Computers and Law 21(3), 31-33.

Yu, P. (2010) The "graduated response". Florida Law Review, 62, 1373-1430.

Internet

Anderson, N. (2008) RIAA "graduated response" Plan: Q&A with Cary Sherman. Online at http://arstechnica.com/old/content/2008/12/riaa-graduated-response-plan-qa-with-cary-sherman.ars. Accessed: 23.01.2011

Anderson, N. (2009a) Irish ISP Agrees to Disconnect Repeat P2P Users. Online at http://arstechnica.com/telecom/news/2009/01/irish-isp-agrees-to-disconnect-repeat-p2p-users.ars. Accessed: 03.02.2011

Anderson, N. (2009b) Verizon to Forward RIAA Warning Letters (but that's all). Online at http://arstechnica.com/tech-policy/news/2009/11/verizon-to-forward-riaa-warning-letters-but-thats-all.ars. Accessed: 13.02.2011

Anderson, N. (2010) Cor blimey! British ISPs Must Fund P2P Copyright Crackdown Online at http://arstechnica.com/tech-policy/news/2010/09/should-isps-pay-for-p2p-warning-letters-uk-says-yes.ars. Accessed: 01.02.2011

Arthur, C. (2011) ACS: Law and MediaCAT Close Their Doors, Ending File sharing Claims. Online at http://www.guardian.co.uk/technology/blog/2011/feb/04/acs-law-mediacat-close-filesharing. Accessed: 07.02.2011

Ashford, W. (2010) ACS Law Hacking a Text-Book Case That Exposes Several Weaknesses. Online at http://www.computerweekly.com/blogs/read-all-about-it/2010/09/acs-law-hacking-a-text-book-ca.html. Accessed: 19.01.2011

Ashton, R. (2010) DEA Goes to Judicial Review. Online at http://www.musicweek.com/story.asp?sectioncode=1&storycode=1043241 Accessed: 15.11.2010

BT Press Release (2011) BT and TalkTalk appeal Digital Economy Act judgment. Online at http://www.btplc.com/News/Articles/ShowArticle.cfm?ArticleID=A057B5E1-1BB3-4751-B208-60EC04E1E348 . Accessed: 01.06.2011

Camphuisen, A. (1999) Telco's ISP ADDS Filter Technology. Online at http://www.internetnews.com/bus-news/article.php/216671/Telcos-ISP-Adds-Filter-Technology.htm. Accessed: 17.03.2011

Cardingham, C. (2008)] £16,000 ($32,000) Fine for First Brit Convicted of Illegal File Sharing. Online at http://www.money.co.uk/article/1001203-16-000-pound-fine-for-first-brit-convicted-of-illegal-file-sharing.htm. Accessed: 12.01.2011

Cellan-Jones, R. (2009) Fact about File-Sharing. Online at http://www.bbc.co.uk/blogs/technology/2009/11/facts_about_filesharing.html. Accessed: 11.03.2011

Cheng, J. (2009) Germany Says "Nein" To Three-Strikes Infringement Plan. Online at http://arstechnica.com/tech-policy/news/2009/02/germany-walks-away-from-three-strikes-internet-policy.ars. Accessed: 26.01.2011

Dickerson, J. and Watson, A. (2010) Commentary by Burges and Salmon [LLP] on The Digital Economy Act, 2010. Online at http://www.burges-salmon.com/Sectors/technology_media_telecommunications/Publications/The_Digital_Economy_Act_2010.pdf. Accessed: 15.02.2011

Du Preez, D. (2011) Government Says ISPs Should Quit Bellyaching about Digital Economy Act. Online at http://www.computing.co.uk/ctg/news/2025804/government-isps-quit-bellyaching-digital-economy-act. Accessed: 15.02.2011

ECJ Press Release (2011) Advocate General's Opinion in Case C-70/10 Scarlet Extended v Société belge des auteurs compositeurs et éditeurs (Sabam) Online at http://curia.europa.eu/jcms/upload/docs/application/pdf/2011-04/cp110037en.pdf. Accessed: 15.04.2011

Edwards, L. (2009) Mandy and Me: Some Thoughts on the Digital Economy Bill. Online at http://blogscript.blogspot.com/2009/11/mandy-and-me-some-thoughts-on-digital.html. Accessed: 14.01.2011

Fiveash, K. (2011) Online at OFCOM to Review Digital Economy Act Site-Blocking Measures. http://www.theregister.co.uk/2011/02/01/OFCOM _reviews_digital_economy_act/. Accessed: 02.02.2011

Fleischer, P. (2007) Are IP Addresses "Personal Data"? Online at http://peterfleischer.blogspot.com/2007/02/are-ip-addresses-personal-data.html. Accessed: 23.03.2011

Forde, E. (2010) France's 'Three Strikes' Law Goes into Action. Online at http://www.musicweek.com/story.asp?storyCode=1042612&sectioncode=1. Accessed: 12.02.2010

Geist, M (2010) Estimating the Cost of a Three-Strikes and You're Out System. Online at http://www.thestar.com/business/article/755443--geist-three-strikes-and-youre-out-system-draw-cries-of-foul-from-governments. Accessed: 11.03.2011

Horten, (2009) HADOPI-2 goes to Constitutional Council . Online at http://www.iptegrity.com/index.php?option=com_content&task=view&id=417&Itemid=9. Accessed: 10.03.2011

Hunton and Williams, (2010) Study on Online Copyright Enforcement and Data Protection in Selected Member States, European Commission, DG Internal Market and Services. Online at http://ec.europa.eu/internal_market/iprenforcement/docs/study-online-enforcement_042010_en.pdf. Accessed: 14.02.2011

Killock, J. (2010) The future of the Digital Economy Act is in Your Hands. Online at http://www.openrightsgroup.org/blog/2010/the-future-of-the-digital-economy-act-is-in-your-hands. Accessed: 10.02.2011

La Rue, F. (2011) Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. Online via http://torrentfreak.com/un-disconnecting-file-sharers-breaches-human-rights 110603/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Torrentfreak+%28Torrentfreak%29. Accessed: 07.06.2011

Leppla, F. (2010) Tens of Thousands Could Be Priced Out of Broadband After Government Announcement on File Sharing Code. Online at http://www.openrightsgroup.org/blog/2010/tens-of-thousands-could-be-priced-out-of-broadband-after-government-announcement-on-file-sharing-code. Accessed: 04.02.2010

Llewellyn, H. (2009) 'Three-Strikes' Off Anti-Piracy Agenda in Spain. Online at http://www.billboard.biz/bbbiz/content_display/industry/e3i8071e0d9c25cb6b876d3771fb7e3d102. Accessed: 02.01.2011

Lovejoy, N. (2011) Procedural Concerns with the HADOPI "graduated response" Model Online at http://jolt.law.harvard.edu/digest/copyright/procedural-concerns-with-the-HADOPI-graduated-response-model. Accessed: 15.01.2011

Mann, A. (2010) The Digital Economy Bill. Online at http://www.bristows.com/?pid=46&nid=1491&level=2. Accessed: 22.01.2011

Moya, J. (2010) Finland Makes Internet Access a Fundamental Right. Online at http://www.zeropaid.com/news/89772/finland-makes-internet-access-a-fundamental-right/. Accessed: 23.03.2011

Petrou, A. (2010) Coalition Government U-turns on repealing Digital Economy Act. Online at http://www.techeye.net/internet/coalition-government-u-turns-on-repealing-digital-economy-act>. Accessed: 14.02.2011

Pilcher, P. (2010) So long Section 92A - New Copyright Bill Revealed. Online at http://www.nzherald.co.nz/technology/news/article.cfm?c_ id=5&objectid=10628193>. Accessed: 22.01.2011

Singel, R. (2008) Internet Mysteries: How Much File-sharing Traffic Travels the Net? – Update. Online at http://www.wired.com/threatlevel/2008/05/how-much-file-s/. Accessed: 20.12.2010

Sroussi, G. (2009) France - The HADOPI Law and France's Controversial Fight against Piracy. Online at http://www.linklaters.com/Publications/Publication1403Newsletter/20091016/Pages/FranceTheHADOPILaw.aspx . Accessed: 14.02.2011

Strowel, A. (2009) Internet Piracy as a Wake-up Call for Copyright Law Makers - Is the "graduated response" a Good Reply? The WIPO Journal, 2009 Issue: 1. pg; 83-94 Online at http://www.world-intellectual-property-organization.com/about-wipo/en/pdf/wipo_journal.pdf. Accessed: 23.01.2011

Topware Interactive v Barwinska. (2008) Patents County Court's Partial Copy of the Order (PAT-08023) Online at http://beingthreatened.yolasite.com/resources/Beschluss%20Topware%20Interactive%20INC.pdf. Accessed: 01.02.2011

TorrentFreak, (2010) France Starts Reporting 'Millions' of File-Sharers. Online at http://torrentfreak.com/france-starts-reporting-millions-of-file-sharers-100921/#. Accessed: 22.01.2011

TorrentFreak, (2011) RIAA Labels Spain and Canada as Piracy Havens. Online at http://torrentfreak.com/riaa-labels-spain-and-canada-as-piracy-havens-110217/. Accessed: 17.02.2011

Williams, C. (2010) High Court to probe Digital Economy Act. Online at http://www.theregister.co.uk/2010/11/10/bt_talktalk_digital_economy/. Accessed: 22.01.2011

Official Publications [Online]

Article 29 Data Protection Working Party (2007) Opinion 4/2007 on the Concept of Personal Data. Online at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf. Accessed: 30.03.2011

BIS (2010) HM Government Response to the Consultation on Online Infringement of Copyright (Initial Obligations) Cost Sharing Online at http://www.bis.gov.uk/assets/biscore/business-sectors/docs/o/10-1131-online-copyright-infringement-government-response. Accessed: 14.02.2011

Carter, S. (2009) The Digital Britain Report Online at http://webarchive.nationalarchives.gov.uk/+/http://www.culture.gov.uk/images/publications/digitalbritain-finalreport-jun09.pdf. Accessed: 02.12.2010

Digital Economy Act, 2010. Chapter 24. Online at http://www.legislation.gov.uk/ukpga/2010/24/data.pdf. Accessed: 03.01.2011

DSI - Draft Statutory Instrument (2011 No. 0000) The Online Infringement of Copyright (Initial Obligations) (Sharing of Costs) Order 2011. Online at http://www.legislation.gov.uk/ukdsi/2011/9780111505779/contents. Accessed: 25.01.2011

Gowers Report, (2006) Online at http://www.officialdocuments.gov.uk/document/other/0118404830/0118404830.pdf. Accessed: 01.02.2011

Information Commissioner Office (ICO) (2010) Data Protection: Personal information Online – Code of Practice. Online at http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Detailed_specialist_guides/personal_information_online_cop.ashx. Accessed: 22.02.2011

Parliamentary Debate, (2010). The Digital Economy Bill Online at http://www.parliamentlive.tv/main/player.aspx?meetingid=6118&st=15:28:3. Accessed: 20.03.2011

UN General Assembly Human Rights Council Report (2011) Online via http://torrentfreak.com/un-disconnecting-file-sharers-breaches-human-rights 110603/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Torrentfreak+%28Torrentfreak%29. Accessed: 07.06.2011

Podcast

Walden, I. (2011) Investigations & Enforcement: The Role of Internet Service Providers http://www.cpdcast.com/podcasts/investigations-and-enforcement-the-role-of-isps