INTERNET SERVICE PROVIDERS' MONITORING OBLIGATIONS: RECENT DEVELOPMENTS

by

EBENEZER DUAH*

Since 2004, legislation or courts in Europe have insistently required internet service providers (ISPs) to play various roles in the fight against online copyright infringement. Some of the obligations being placed upon the ISPs have included the disclosure of subscribers' personal data, the filtering and blocking of access to infringing content or committing to sustained cooperative regulatory policies such as a graduated response mechanism. Although such approaches may be aimed at controlling illicit file-sharing, the trends being pursued by the copyright holders are also to be seen by ISPs as a move from their "passive-reactive roles" towards "active-preventative" roles. Particularly, the scope of ISP obligations are increasingly being seen as blurred and this has prompted several legal challenges in the courts with some of the litigations ended at the national levels and others required the intervention of the European Court of Justice. This paper will examine the extent to which the monitoring obligations placed upon the ISPs have been interpreted and assess the possible implications for the fight against file-sharing.

KEYWORDS

Internet service providers, Monitoring, Injunction, Filtering, Peer-to-peer, File-sharing, Directive, Copyright, Blocking, General obligation

1. INTRODUCTION

It is not unusual for internet intermediaries such as internet service providers (ISPs) to conduct monitoring or blocking of certain information in the course of its business.[1] One of the common methods used has been Deep

* Ebenezer Duah. Aberystwyth University, UK. <E-mail: ead09@aber.ac.uk>

Packet Inspection (DPI)[2] which is regarded among the network communities as capable of addressing various internet governance challenges including malware problems[3] and the optimisation and monetisation of commerce.[4] The reliance on DPI has also been based on its efficiency to manage and apportion bandwidth for network operators. In other cases monitoring obligations have been essential to enable the blocking of access to undesirable content. Although, libellous, defamatory or pornographic content formed the basis of liability of online intermediaries on the internet in earlier years[5], copyrighted content appears to be shifting the focus. In recent years ISPs are increasingly being asked by the courts and governments to play more active policing roles on their networks so as to tackle online copyright infringement. There are several reasons why ISPs can be attractive for regulatory interventions one of which lies in their size. They are often bigger than the actual wrongdoer and are easily identified. As also supported by the preamble to the Copyright Directive,[6] services such as ISPs are best placed to bring infringing activities to an end and in addition, it is relatively cost effective to pursue ISPs rather than the millions of file-sharers. To accomplish such goals, the usual enforcement 'routes' have been either through litigations or legislations such as the graduated response mechanisms (GRM)[7], both of which may be aimed at; (1) the possibility of sanctions against ISPs to force them to tackle infringement carried out on their networks by third parties; (2) obligations to promptly inform rights holders of alleged illegal activities upon request and; (3) the right to apply

---

1 Catharine Lumby, et al 'Untangling the Net: The Scope of Content Caught by Mandatory Internet Filtering'. SCRIBD <http://www.scribd.com/doc/24138351/Untangling-the-Net-The-Scope-of-Content-Caught-by-Mandatory-Internet-Filtering> (Accessed: 30 October 2011)

2 Deep packet inspection (DPI) is a technology for scanning and analyzing Internet traffic and making decisions about how to handle it in real-time

3 Sunil Kim & Jun-Yong Lee. 'A system Architecture for High-Speed Deep Packet Inspection in Signature-Based Network Intrusion Prevention.' Journal of Systems Architecture. vol 53, no 5-6, pp. 310-320.

4 Armen Aghasaryan, et al. 'Personalized Application Enablement by Web Session Analysis and Multisource User Profiling.' Bell Labs Technical Journal. vol 15 no 1, pp. 67-76.

5 Lilian Edwards, 'Defamation and the Internet and Pornography and the Internet' in Lilian Edwards and Charlotte Waelde (Eds). Law and the Internet: A Framework for Electronic Commerce. (Hart Publishing 2000)

6 Recital 59 of Directive 2001/29/EC of the European Parliament And of the Councilof 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (InfoSoc Directive) [L 167/10]

7 A "graduated response mechanism" or a "three strikes and you are out" is a legislative approach which imposes an obligation on ISPs to notify subscribers of copyright infringements occurring with their account and the possibility of their account being suspended or cut off if they do not desist.

to a court for relief against ISPs to prevent infringement of rights. While the "routes" mentioned above are not exhaustive, they raise concerns and possible conflicts with legislative safeguards awarded service providers[8], and impact on the applicable fundamental rights of internet users. The paper begins by examining the intermediary immunities under the Electronic Commerce Directive; then moves onto assess the monitoring obligations placed upon them from different angles before gauging their impact on the fight against file-sharing.

2. INTERMEDIARY IMMUNITIES

For an ISP within Europe, immunities from liabilities can be found within Articles 12 to 15 of the ECD[9], which deals with exemptions for acting as a mere conduit[10] for merely caching[11] or hosting information.[12] Art. 12 covers 'mere conduits' engaged in either the transmission of the information provided by the recipient of the service or access provision to a communication network, while Art. 13 also deals with the automatic, immediate and temporary storage of information, performed for the sole purpose of making more efficient the information's onward transmission. Art. 14 then deals with hosts of online materials. It is safe to say that, the primary and possibly the only target for the first two immunities described above are for access providers which will include Scarlet, British Telecom (BT) or TalkTalk, while Art. 14 targets content hosts and Web 2.0 providers, one example being social networking sites. With the high volume of transmissions that occur across an ISP network, the various immunities appear reasonable as without them, it could be almost impossible for ISPs to provide a smooth service.[13] While internet intermediaries might have hoped that these defences are absolutely protected, there are conditional clauses that apply such as an ISP neither selecting nor modifying the information being trans-

---

[8] Arts 12-15 of Directive 2000/31/EC Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (E-Commerce Directive-ECD) [L 178/1]

[9] E-Commerce Directive (ECD)

[10] ECD, art. 12

[11] ECD, art. 13

[12] ECD, art. 14

[13] See Pablo Baistrocchi (2003) Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce, 19 Santa Clara Computer & High Tech Law Journal. Vol 19, pp. 111-130 (2002-2003), [126]

mitted[14] or to comply where the notice-and-takedown (NTD) regime[15] is invoked.[16] Aside from the NTD, the scope of ISP liabilities could further be unspecified as the immunities shall not affect the possibility of a court or administrative authority … of requiring the service provider to terminate or prevent an infringement.[17] It seems then that the basic principles applicable to internet intermediaries can therefore be summed up as that; in most cases, access providers by acting as mere conduits may be exempted from liability provided they abide by the conditions within the provisions; that if they are acting as a mere conduit, they are unlikely to be liable for direct copyright infringement; that hosting service providers are not liable for monetary relief in the absence of knowledge or control; and will also not be liable for monetary relief if they immediately disable access to the infringing content upon acquiring knowledge or awareness. Except that, a court or administrative authority can also require the termination or prevention of an infringement further blurring the scope of such immunities.

A recent test case to determine the scope of an ISP liability for copyright infringement conducted by its users was the Australian case of *Roadshow Films v iiNet*,[18] which concerned whether the ISP, iiNet, had authorised infringements of its subscribers. The Trial Court ruled that iiNet cannot be held liable for its subscribers' illegal movie downloading by means of the BitTorrent P2P system[19] as it had not authorised any infringements; had no control over the infringing activities; and had adequately complied with procedures to qualify for immunities. But the applicants appealed,[20] through to the High Court[21] who delivered its verdict in April 2012, by upholding the previous rulings and hence found in favour of the defendant ISP.[22] The Courts' position illustrates the extent to which an ISP safe har-

---

[14] ECD, art. 12(1)

[15] A notice-and takedown regimes usually relates to the copyright owners' informing of the availability of , access to a protected work on an ISP network unlawfully and requesting that the service provider takes appropriate steps to remove or disable access to the content.

[16] ECD, arts 13(1e) and 14(1b)

[17] See ECD, arts 12(3), 13(2), 14(3)

[18] [2010] FCA 24

[19] BitTorrent is one of the protocols for transferring large files.

[20] [2011] FCAFC 23

[21] John Hannebery and Miriam Zanker 'Roadshow Films appeals iiNet Copyright Decision to the High Court' <http://www.davies.com.au/pub/detail/417/roadshow-films-appeals-iinet-copyright-decision-to-the-high-court> (Accessed: 11 November 2011).

[22] See 'iiNet: ISP Not Liable For BitTorrent Piracy, High Court Rules' Online at, http://torrentfreak.com/iinet-isp-not-liable-for-bittorrent-piracy-high-court-rules-120420/ (Accessed: 01 May 2012)

bour based on subscribers' infringing activities could be determined and particularly the courts showed that providing access to the internet and providing the means of infringement could not be the same, if control cannot be established.

Immunity for hosts providers have perhaps been the most controversial of the immunities. Rowland et al, state that, "on the primary intermediary spectrum it comes closest to the dividing line between the two immunities above due to the part it plays in the publishing process which may undermine its status as a neutral, and therefore innocent, immunity-deserving middleman".[23] Hence in order to qualify under this provision, it must be established that the intermediary does not authorise or control the third party. The ECJ in the *Google Adwords* case[24] extended this scope by taking into account the extent of the service provider's passive or neutral conduct in determining the liability exemption under Art. 14.

3. MONITORING OBLIGATIONS

Beyond the strict liability offences, the immunities outlined above, also capture negligence based offences,[25] as any NTD must be read in conjunction with general obligations on service providers to monitor their networks.[26] While monitoring in specific cases is allowed[27] Member States are to refrain from imposing on ISPs a general obligation on providers to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity. With the background so far, the issue to begin with, is to what extent will the right of court to issue an injunction to prevent infringements intrude on the obligations on Member States not to impose general monitoring obligations on an ISP?

4. LITIGATIONS

One of the cases that focused on finding an answer to this issue began in Belgium. It was the case of *SABAM v S.A. Tiscali (Scarlet)*,[28] brought by the

---

[23] Diane Rowland, et al. 'Information Technology Law' [4th Edn] (Routledge 2012), 85

[24] [2010] EUECJ C-238/08

[25] Rowland (n23)

[26] Art. 15(1) of Directive 2000/31/EC provides that Member States shall not impose a general obligation on providers, when providing the services covered by Arts 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.

[27] Recital 47 of ECD

[28] [2007] E.C.D.R. 19

Belgian Society of Authors, Composers and Publishers (SABAM) who in 2004 had applied for an interim relief against the defendant ISP Scarlet, alleging that Scarlet knowingly permitted the infringement of its members' protected works through peer-to-peer (P2P) file sharing over the ISP network. In particular, SABAM sought an order[29] requiring the filtering and blocking of SABAM's repertoire being downloaded or shared over the defendant's network without permission. In an interlocutory judgement, SABAM was thought to posses the grounds for granting such an order except that the court still needed more clarity on a technical feasibility and enlisted the services of a technical expert.[30] The technical expert report had recommended a filtering system called CopySense[31] developed by Audible Magic as the filtering solution capable of specifically responding to the problem,[32] although the report was also cautious about the long-term effectiveness due to possible circumvention.[33] But the trial Court appeared satisfied with the report and the submissions by SABAM and ruled against ISP Scarlet[34] rejecting the defendant's argument that the order would impose a general obligation on it to monitor all traffic and result in losing the benefit of the mere conduit exemption under Art12.[35] In the court's reasoning, the technical deployments would only be confined to the blocking or filtering of certain information transmitted on Scarlet's network only.[36] At that stage, it was to be assumed that the filtering solution at issue does (or will) not conduct a detailed analysis nor over-block access by its implementation.[37] However, while it was not technically feasible to comply with the order, Scarlet appealed to the Court of Appeal to set aside the lower Court's judgment and make a fresh ruling on the original claims. But before rendering its judgement, the Court of Appeal then forwarded two questions to the

---

[29] Injunction pursuant to Art. 87(1) of the Belgian Copyright Act as interpreted in the light of Directive 2001/29/EC and Directive 2004/48

[30] Fran Mady, et al 'Translation Series: Sabam v. S.A. Tiscali (Scarlet), District Court of Brussels, 29 June 2007' <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1027954> (Accessed: 11 October 2011)

[31] Audible Magic's CopySense is a network appliance product, which examines network traffic at the content layer, that is, analyzes the actual file transferred in an application-layer transaction

[32] Ibid (n28) [15]-[16]

[33] Technical expert had noted that advances in technologies could circumvent the implementation.

[34] Ibid (n 28), 19

[35] Ibid [25]

[36] Ibid [32]

[37] [2011] EWHC 2714 (Ch) [6]

ECJ seeking a preliminary ruling.[38] The answers to these questions came in November 2011, when the ECJ ruled that the contested system will have to filter all communication traffic in order to block infringing files which will constitute a general obligation to monitor. [39] Consequently, it will also place restrictions on the right to respect for the privacy of communications and the right to protection of personal data, both of which are protected under the Charter of Fundamental Rights.

It does suggest that the Belgian Trial Court perhaps attempted to make clear the normal issues relevant to any injunction such as efficacy and feasibility without adequately balancing the magnitude of harm to the copyright owner against the burden on the ISP, not least in respect of the general obligation under the Enforcement Directive.[40]

As with the pursuit against Scarlet, SABAM had also asked for a similar broad injunction against Netlog,[41] at a Belgian Court which also eventually ended up at the ECJ for guidance. The questions to the ECJ in Netlog were based on whether EU law and the fundamental rights to privacy and freedom of expression allowed national courts to issue injunctions to impose such a filtering system. In its ruling,[42] the ECJ seemed to have repeated its reasoning and arrived at the same conclusion as in Scarlet.[43] While Scarlet is an ISP, and Netlog is a an online social networking site, the differences in the service provision might have had consequences with the application of law given that an ISP could typically be providing access and not store any information, and even if it temporarily did (in the cause of transmission) would be shielded from liability within the meaning of Art. 12 of the ECD.[44]

---

[38] The question sent to the ECJ for answers were whether European Union (EU) law and, in particular, the fundamental rights guaranteed by the Charter of Fundamental Rights, permits national judicial authority to order an Internet Service Provider to introduce, for all its customers, in abstracto and as a preventive measure, … a system for filtering all electronic communications, both incoming and outgoing, passing via its services … in order to identify on its network the sharing of electronic files containing a musical, cinematographic or audio-visual work in respect of which the applicant claims to hold rights, and subsequently to block the transfer of such files, either at the point at which they are requested or at which they are sent …".

[39] [2011] EUECJ C-70/10

[40] Art. 3 of Directive 2004/48/EC states that Member States shall provide for measures, procedures and remedies necessary to ensure the enforcement of intellectual property rights which must be fair and equitable, not necessarily complicated and costly, and not entail unreasonable time-limits or unwarranted delays.

[41] Netlog is a social networking site that operates in Belgium.

[42] [2012] EUECJ C-360/10

[43] Ibid (n 39)

[44] See Philippe Laurent, P. 'SABAM v. Netlog (CJEU C 360/10) … as Expected!' [Kluwer Copyright Blog, 20 February 2012] <http://kluwercopyrightblog.com/2012/02/20/sabam-v-netlog-cjeu-c-36010-as-expected/> (Accessed: 23 February 2012).

Netlog arguably stores information provided by the users on its servers[45] within the meaning of Art. 14. Nonetheless, Art. 15 of the ECD are vague on any distinction between ISPs and hosting services providers, hence the type of platform may not have influenced the ECJ decision. The main consideration here is that, while the 'Netlog' injunction had been sought on the basis of the Infosoc directive and enforcement directive[46] both directives also provide that the liability exemptions in Arts. 12 to 15 of the ECD are respected.[47] Hence the ECJ found that the basis of the claim would similarly involve invasive analysis of the contents of data packets[48] in breach of Art. 15(1).[49] German Courts have also not relented in their pursuit against infringing websites such as Rapidshare. In a recent ruling, and also taking into account an earlier court ruling which placed obligation on Rapidshare to monitor the copyright status of all works made available on its site,[50] it insisted that the website must take proactive steps to tackle copyright infringement. At a time when the ECJ has also ruled that access providers and host providers cannot be forced by national courts into broadly filtering internet users' activity to identify copyright infringing material, it therefore provides further uncertainties as to which rights may be breached by the website's compliance. Nonetheless, the UK High Court decision in *Twentieth Century Fox v BT*[51] which granted an injunction against BT seemed to a large extent, to be carefully weighed so as to preserve Art. 15 of the ECD as the Court had taken into account the need for the recommended filtering system not to be capable of conducting a detailed analysis and over-block traffic.[52] In rejecting challenges advanced by the respondent that the order would constitute a general monitoring obligation, it had also relied on the guidance in *L'Oréal v eBay*[53] to conclude that the ISPs monitoring obligations will be more specific rather than general in nature, although the extent of a possible conflict with innocent third parties were yet to be determined.

---

45 Laurent (n 44)

46 Basis of Netlog injunction: Art. 8(3) of Infosoc Directive and Art. 11 of Enforcement Directive.

47 See for example Enforcement Directive, art. 2(3).

48 See [2011] EWHC 1981 (Ch.) [167]

49 Netlog (n42)

50 See Out-law News at http://www.out-law.com/en/Art.s/2012/march1/rapidshare-ordered-to-pro-actively-prevent-users-linking-to-identified-pirate-content/

51 Ibid (n 48).

52 [2011] EWHC 2714 (Ch.) [6]

53 C-324/09 L'Oréal [2011] E.T.M.R. 52

5. LEGISLATIONS

With concerns growing over the effectiveness of existing file-sharing strategies,[54] new legislations are being passed or existing laws amended so as to place more obligations on ISPs to contain the problem. Recently the Spanish Sinde Act[55] has been passed and a proposed amendment to the Irish Copyright and Related Rights Act, 2000[56] also advanced to provide owners with the explicit right to obtain an injunction against ISPs.

But the most popular and equally controversial scheme has been what is commonly referred to as the "graduated response model" (GRM) or "three strikes" approach[57] now being proposed, and/or implemented in several jurisdictions. Whether by administrative and ministerial order;[58] by judicial determination supported by administrative bodies or by legislatively supported industry code[59], the general commitment within a GRM begins with the gathering of evidence through the harvesting of alleged infringers' internet protocol (IP) addresses, the notification of alleged infringement by their respective ISPs and internet traffic management to include internet suspension or disconnection for repeat infringers

The French HADOPI law[60] passed in 2009 to implement a GRM involves detection by the copyright owners of potential infringements to be reported to the HADOPI administrative authority. The HADOPI authority then consults with other parties involved, and if contented, contacts the relevant ISPs to seek the identification of these alleged infringers,[61] while also requiring the ISP to send the first notification to the matched subscriber.[62]

---

54 IFPI Digital music Report (2010)

55 See 'Spanish Sinde law Brings About the First Website Take Down Requests' at <http://www.edri.org/edrigram/number10.7/sinde-law-takedown-requests>.

56 See information on draft proposal at <http://www.djei.ie/press/2012/20120126a.htm>.

57 A "graduated response mechanism" or a "three strikes and you are out" are measures which generally require an ISP to take some action against subscribers suspected of copyright infringement: ranging from notification of alleged infringement with the account, keeping records of allegations made against subscribers and alerting copyright owners, to account suspension and termination of service.

58 Heesob Blog, 'Facts and Figures on Copyright Three-Strike Rule in Korea'. Online at <http://hurips.blogspot.com/2010/10/facts-and-figures-on-copyright-three.html> (Accessed:22/01/2012)

59 Example being the Digital Economy Act 2010, s. 3-18.

60 Passed in 2009 to provide a graduated response as a means to encourage compliance with copyright laws and HADOPI is the acronym of the government agency created to administer it.

61 May, B. and Liens, M. (2009) France's Attempt to Introduce Anti-Piracy Legislation.

62 Lovejoy '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 January 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.[63] 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 along with the option of subscribers appeal.[64] On the face of it, although the account holder is to comply with his obligation to monitor his own account,[65] ISP will be tasked with monitoring at various stages in the process, not least when technical measures are introduced to manage serial infringers' accounts. Arguably, based on the guidance in *L'Oréal*, such monitoring may qualify as a specific rather than a general obligation. With slight variations in the French model, the UK GRM legislation under its Digital Economy Act DEA, 2010[66] is of particular interest as the Courts have had to decide on whether the contested provisions placed any monitoring obligations on the ISP while the draft obligations code is being finalised. As a background, the UK model entails an initial obligation, technical obligation and a website blocking provision. The initial obligations require ISPs to act upon the infringement report received from copyright holders by warning respective subscribers of alleged infringement occurring with their accounts.[67] While it also places upon them the obligations to design and maintain a copyright infringement list (CIL) of serial infringers to be handed over to the rights holders upon request so as to pursue a legal action.[68] The technical obligation when introduced may lead to internet account management in varying degrees including internet speed slowdown and the suspension of a subscribers' account.[69] Concerns raised by the ISPs led to a judicial review of the DEA in the case *BT v The Secretary of State*[70] and among the grounds of challenges advanced was the potential breach of immunities under the ECD. Claimants had submitted that the obligations will require

[63] Ibid

[64] See Grégory Sroussi 'France - The HADOPI Law and France's Controversial Fight against Piracy. <http://www.linklaters.com/Publications/Publication1403Newsletter/20091016/Pages/FranceTheHADOPILaw.aspx .> (Accessed: 14 February 2011).

[65] Decrees No. 2010-695 dated 25 June 2010 (OJ 26 June 2010, at 11536).

[66] The Digital Economy Act 2010 (c. 24) is an Act of the Parliament of the United Kingdom regulating digital media.

[67] Communications Act (CA) 2003 s 124A

[68] Ibid

[69] Ibid [124G (3)]

[70] [2011] EWHC 1021

them to monitor the information transmitted by subscribers, and also retain that information and monitor all other CIRs notified in respect of the same subscriber. Whereas technical measures may also "give rise to a de facto form of real time monitoring, based on internet usage over a period of time".[71] The judicial review judgement found nothing in the initial obligations code as constituting a general obligation on the claimants (ISPs) to monitor any information, nor a general obligation to actively seek facts or circumstances indicating illegal activity.[72] In the High Court's reasoning, the data to be handled by the ISPs[73] would be nothing more than merely reporting to the subscriber, information received from the right holders of alleged infringement which is legally permissible. While the maintenance of the infringement list by ISPs, within the meaning of 124B CA, 2003, would also amount to a mere compilation of CIRs in respect of a repeat infringer[74], rather than an obligation to monitor that information. In the Court's interpretation, right holders have rather been the parties who actively seek facts and circumstances indicating illegal activity through the harvesting of IP addresses of alleged infringers,[75] hence engaged in monitoring. In March, 2012, the UK Court of Appeal[76] also found the DEA not in breach of EU laws, after indicating that the balance struck by the DEA was about right,[77] although it is the case that the High Court interpretation of Art. 15 meant that the Court of Appeal did not give permission on that point.[78] So far, the Courts have found no need to address any potential conflict posed by technical measures as the introduction of any 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.[79] A clause equally controversial had been s. 17 of the DEA which allows for the making of provision about injunctions preventing access to locations on the internet. In summary, it had been feared that, it would provide broad injunc-

---

[71] The DEA Challenge, 'A copy of the Statement of Facts and Grounds filed at Court by BT and TalkTalk'. < http://www.btplc.com/newsadmin/attachments/statement%20of%20facts%20and%20grounds.pdf> (Accessed: 12 May, 2011), pp. 44

[72] Ibid (n 70)

[73] Ibid

[74] Ibid [118]

[75] Ibid [116-118]

[76] [2012] EWCA Civ 232

[77] Ibid [46]

[78] [2011] EWCA Civ 1229 [20]

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

tions and would be open to abuse or misuse. While the controversy appears to have faded as the UK Government has indicated that it is unlikely to use this provision in the foreseeable future,[80] existing provisions under UK copyright law has resulted in ISPs being ordered by the Courts[81] to implement technical measures to monitor and block their users' access to infringing websites.[82] These developments still raises concerns about the overall impact on other stakeholders, not least the impact upon innocent third parties.

6. VOLUNTARY SCHEMES

Also being developed are voluntary (or potential) schemes which are modelled through contractual agreements between the ISPs and subscribers, or other proposed instruments capable of by-passing judicial oversight. They are often proposed and implemented where governments are unwilling to legislate or where there may not be the legal basis upon which a national court could grant a relief.[83] The *EMI v Eircom*,[84] is an example of a voluntary GRM scheme based on end-user contractual agreements which the court ruled as lawful so as to protect copyright online, but practically potential conflicts with aspects of users rights have always raised concerns. There have also been quite lot of debates about the Anti-Counterfeiting Trade Agreement (ACTA)[85] and online copyright infringement. Although, it is only a proposed legal instrument, the potential impact can be envisaged. Particularly Art 27 of ACTA imposes an obligation on States to support "cooperative efforts with the business community" in order to enforce criminal and civil law in the online environment.[86] This means that the scale and extent of such measures can be decided upon by private companies without the need for any judicial scrutiny. While, the lawfulness of such orders in the European sense have (and could see) the intervention of its highest

[80] Out-Law News 'New Website Blocking Regulations not on The Agenda, Government says'.< http://www.out-law.com/page-12129> (17 February 2012).

[81] Implemented in the UK by s. 97(A) of the CDPA 1998

[82] See Dramatico Entertainment Ltd & Ors v British Sky Broadcasting Ltd & Ors [2012] EWHC 1152 (Ch.)

[83] See EMI v UPC [2010] E.C.D.R. 17

[84] [2010] IEHC 108

[85] The Anti-Counterfeiting Trade Agreement (ACTA) is a multinational treaty for the purpose of establishing international standards for intellectual property rights enforcement.

[86] See 'ACTA Fact Sheet' Online at, http://www.edri.org/ACTAfactsheet.

Court so as to protect the rights of the end-user, voluntary agreements can therefore be illegally implemented outside the law.

7. IMPACT ON THE FIGHT AGAINST FILE-SHARING

Now how will the discussions impact on the fight to control file-sharing? What has emerged is that a broad injunction against a service provider to deploy filtering systems may constitute a general monitoring obligation, in breach of the ECD. It also established that by the active monitoring of all the data relating to each of its customers, it would not respect the rights of internet users. In any case, it must also be pointed out that it will also depend on the court's determination of the order and the exact capabilities of the recommended technology. Judging by the arguments raised be the GRM model, there appears to be the indication that at least the initial obligations are less likely to entail general obligation on ISPs to monitor and hence may see ISPs sending warning letters to their subscribers and also keeping records of infringements. In terms of the likely implications on the fight against file-sharing, it could be said that the ECJ guidance[87] limit service providers' responsibility to filter and block in the sense that it essentially clarifies the generalised efforts to require the filtering of all communications on networks to identify copyright infringing material and prevent transmissions is not legally permissible. This invariably also sets boundaries around the future implementation of technical measures to be required of the ISPs. While, the obligations could still be contested further, what has not gained much attention in the debate is about finding a middle ground to engage with all the stake holders where copyright could be protected while the rights are also respected. Perhaps the concept of notice-to-notice (NTN) could be one way of easing the uncertainties still associated with a GRM model. In a NTN system, a notification is also made by the copyright holder to the relevant ISP about an infringement by an account holder. The ISP will only forward the notification to the subscriber but takes no further action. Neither will it remove the content from the system, disclose subscriber's personal data or terminate subscriber's internet accounts. It falls to the subscriber to act voluntarily which some evidence suggests will see compliance by consumers where the content is infringing.[88] This is believed that unlike

[87] Ibid (n 39), ibid (n 42).

[88] See; 'Canada's Notice-and-notice'. <http://www.p2pnet.net/story/11344> (Accessed 30 April, 2012).

NTD which could lead to potentially non-infringing content also taken down,[89] the NTN approach protects user privacy.

8. CONCLUSION

In reviewing the litigations, and legislative approaches, a number of observations have been made. While the strategies identified in the paper seek compliance from ISPs to tackle online copyright infringement, , ISPs' defences requiring it to notify subscribers' of alleged infringements appear weak, except that there is the indication that Art.15 of the ECD also gradually being preserved by some court decisions. This is to say that, the courts have been very particular not to breach this provision by taking into account the capabilities of any recommended technical measures in relation to users' rights. Where these have been considered, the follow-on effects have also been the tacit perception of both the InfoSoc Directive and ECD at least complementing each other instead of the former superseding the latter. Given that the ECJ judgements discussed ruled on the permissible scope of the injunction, they set important limits on what technical measures may or may not be implemented irrespective of whether they are set through litigation or legislation as examined in the light of this paper. What is still unclear is the potential impact that voluntary agreements may have on both ISPs obligations and users' fundamental rights where orders could be implemented outside of the law.

REFERENCES

[1] Aghasaryan, A. et al. 2010, 'Personalized Application Enablement by Web Session Analysis and Multisource User Profiling.' Bell Labs Technical Journal vol 15, no 1, pp. 67-76.

[2] Angelopoulos, C. 2009, 'Filtering the Internet for Copyright Content in Europe'. Available online at, <http://www.obs.coe.int/oea_publ/iris/iris_plus/iplus4_2009.pdf.en> (Accessed: 02 November, 2011)

[3] Baistrocchi, P. 2003, Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce. 19 Santa Clara Computer & High Tech Law Journal. Vol 19, pp. 111-130 2002-2003

[4] CoE, 2008, Council of Europe, Report by the Group of Specialists on Human Rights in the Information Society (MC-S-IS) on the Use and Impact of

[89] See Greg Sandoval. 'EFF takes Viacom to Task over YouTube Takedown' <http://news.cnet.com/EFF-takes-Viacom-to-task-over-YouTube-takedown/2100-1026_3-6159548.html> (Accessed:20 April 2012)

Technical Filtering Measures for Various Types of Content in the Online Environment. [CM (2008)37]

[5] Edwards, L & Waelde, C. 2000, 'Law and the Internet: A Framework for Electronic Commerce'. Hart Publishing, UK

[6] Farrand, B. 2010, 'The Digital Economy Act 2010: A Cause for Celebration, or a Cause for Concern?' European Intellectual Property Review, 2010, vol 32, no 10, pp. 536-541

[7] Heaney, A. 2010, 'Response to paper by Birgitte Andersen on the Digital Economy Act'. Prometheus, vol 28, no 4, 2010, pp. 395-399

[8] Hannebery, J & Zanker, M. 2011, 'Roadshow Films appeals iiNet Copyright Decision to the High Court'. Available online at, <http://www.davies.-com.au/pub/detail/417/roadshow-films-appeals-iinet-copyright-decision-to-the-high-court> (Accessed: 11 November 2011).

[9] Laurent, P. 2012, 'SABAM v. Netlog (CJEU C 360/10) … as Expected!' Available online at, <http://kluwercopyrightblog.com/2012/02/20/sabam-v-netlog-cjeu-c-36010-as-expected/> (Accessed: 23 February, 2012)

[10] Lumby, C., Green, L., and Hartley, J. 2009, 'Untangling the Net: The Scope of Content Caught by Mandatory Internet Filtering' Available online at, <http://www.scribd.com/doc/24138351/Untangling-the-Net-The-Scope-of-Content-Caught-by-Mandatory-Internet-Filtering> (Accessed: 30 October 2011)

[11] Kim, S & Lee, J. 2007, 'A system Architecture for High-Speed Deep Packet Inspection in Signature-Based Network Intrusion Prevention.' Journal of Systems Architecture. vol 53, no 5-6, pp. 310-320.

[12] Mady, F., Bourrouilhou, J., & Hughes, J. 2008, 'Translation of the Decision in SABAM v. S.A. Scarlet, District Court of Brussels, No. 04/8975/A, 2007' in 25 Cardozo Arts & Entertainment Law Journal 1279, 2008. Available online at, <http://www.cardozoaelj.net/issues/08/case001.pdf> (Accessed: 14 October, 2011)

[13] Manara, C. 2011, 'Block the Filtering! A Critical Approach to the SABAM Cases' Available online at, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1954760> (Accessed: 20 November, 2011)

[14] Rowland, D., Kohl, U., Charlesworth, A. 2012, 'Information Technology Law' 4th Edition, Routledge, Oxon.

[15] Yu, P. 2010, 'The Graduated Response'. Available online at, <http://www.floridalawreview.com/wp-content/uploads/2010/01/Yu_BOOK.pdf> (Accessed: 17 March 2012)