Developments in Intermediary Liability

Andres Guadamuz[*]

1. Introduction

On February 2005, three PayPal employees, Jawed Karim, Chad Hurley and Steve Chen, attended a San Francisco dinner party, at which they started talking about various topics that included the Asian tsunami and Janet Jackson's wardrobe malfunction at the previous year's Super Bowl. The result of such a random conversation was the idea to create a website in which users could upload videos they wanted to share to the world. On May 2005, the three went ahead and founded a small video-sharing website that later became known as YouTube.[1]

Just over a year after, YouTube had grown to be one of the most important sites in the Internet; by July 2006 the site was receiving 100 million uploads per day and its content accounted for 60% of all videos watched online at the time.[2] The site's popularity was such that Google acquired it in November 2006 for $1.65 billion USD in stock.[3]

While the original intent of YouTube was to provide a platform in which the public would upload their own family events, recorded thoughts, video logs, and other user-generated content, the site was from the start accused of facilitating large-scale copyright infringement.[4] However, despite having clips of TV shows, movies, music videos, and a myriad of other protected content, YouTube managed to avoid being sued for a relatively long period of its early life, which allowed the site to cement its prominent position amongst what was a growing and important sector of the online environment. The reason why YouTube managed to stay on the right side of the law came down to the fact that it was actually protected by copyright legislation. YouTube always claimed that it would cooperate with content owners and that it would remove infringing material. This allowed it to operate within the parameters of existing legislation as an online service provider, protected by the safeguards built into the Digital Millennium Copyright Act (DMCA) in order to shelter intermediaries from litigation.

However, this all changed in March 2007 when media conglomerate Viacom filed a $1 billion USD lawsuit[5] against Google and YouTube alleging direct and indirect

---

[*] Senior Lecturer in Intellectual Property Law, University of Sussex.

[1] Hopkins J, "Surprise! There's a Third YouTube Co-Founder", *USA Today* (October 11, 2006).

[2] Cashmore P, "YouTube Hits 100 Million Videos Per Day", *Mashable* (July 17, 2006), http://on.mash.to/1b0ZTa0.

[3] Arrington M, "Google Has Acquired YouTube", *TechCrunch* (October 9, 2006), v

[4] Fisher K, "YouTube and the Copyright Cops: Safe… For Now?" *Ars Technica* (July 17, 2006), http://ars.to/11F4usZ.

[5] *Viacom International, Inc. v YouTube, Inc.* 2010 WL 2532404 (S.D.N.Y 2010).

copyright infringement. This move by Viacom was surprising given the fact that the law was strongly on the side of Google. Unsurprisingly, Viacom lost the case after a motion for summary judgement was accepted, ruling that YouTube was indeed protected by the DMCA's safe harbor provisions. In other words, as an intermediary online service, YouTube was not liable if it could show that it had a notice and takedown provision for potentially infringing content.

The only surprising element of the whole YouTube saga is that there was a content owner willing to sue them in the first place. From relatively early in the history of Internet regulation, it has been understood that intermediaries should be given some sort of limitation of liability for infringing or illegal content uploaded to a website by its users, as it became evident that many sites did not have the capacity to police content *a priori*. This limitation of liability was set in stone in legislation through international treaties, European Directives and national legislation.

Despite all of the above, in recent years we have witnessed attempt after attempt by content owners to try to hold intermediaries liable in some way or another, first by infringement suits such as Viacom's, to more indirect approaches, such as trying to force intermediaries to filter or block information.

This article looks at the more recent efforts to erode the principles of limitation of liability that have served as the cornerstone of Internet regulation for some years. We will briefly study existing legislation and then we will chart the latest efforts to see the attacks on these limits, particularly by the introduction of graduated response, and the case law that seeks other solutions, such as filtering and blocking.

This area is reasonably harmonised at an international level, so we will take a broad comparative approach. Intermediary liability also covers such different topics as defamation and pornography. The article will try to centre its sights specifically on copyright law, although some other examples will be used where relevant.

2. Don't shoot the messenger

It would be remiss not to provide a description of the current state of the legislation, as it serves to explain the most recent developments. The prevalent limitation of liability for intermediaries arises from the earliest case law, which surprisingly predates the Internet as we know it. Before the popularisation of the World Wide Web, most online services consisted of what is known as Bulleting Board System (BBS),[6] dial-in servers where users could chat, download content and experience many features that would later become the Web. These boards were rife with infringing copyright material, which made them viable targets for litigation, mostly in the US. In some of the earliest cases, the operators of these BBS services were held liable for copyright infringement, mostly because they uploaded the content. In a good number of cases the BBS operators were held liable for facilitating the posting of software owned by the plaintiffs; this

[6] See: http://en.wikipedia.org/wiki/Bulletin_board_system.

happened in litigation such as *Playboy Enterprises v Frena*,[7] *Sega Enterprises v Sabella*[8] and *Sega Enterprises v MAPHIA.*[9]

With the move from BBS to the Internet, case law began to shift, as Internet Service Providers (ISPs) did not have the same level of control over content posted on their servers. While it was easy to hold liable a few hobbyist operators of small and medium scale services for content in their networks, the same was considerably more difficult when the intermediaries did not have editorial control over their systems. We then start to witness cases that show what is to become the norm, as content owners were willing to terminate litigation if the intermediary would remove infringing content. This was the case with software manufacturer Adobe Systems, who dropped two cases against different ISPs when they agreed to remove infringing material and make efforts to stop it from happening again.[10]

The turning point in case law was one of the various Scientology-related pieces of litigation at the time. The Church of Scientology became famous for using copyright law to try to stop critics from posting what it considered to be protected material online that revealed secrets from the organisation. In *Religious Technology Center v Netcom*,[11] customers of Netcom, an ISP that also operated as a BBS, uploaded content that belonged to the plaintiffs to a board hosted by the defendant. The Church of Scientology sued the ISP alleging direct, vicarious and contributory copyright infringement, opening the question of whether an intermediary could be held directly liable for content that had been uploaded by one of its users. The Federal District Court for the Northern District of California ruled that Netcom could not be held directly liable for any infringing material posted by its clients, since Netcom itself did not upload the material. The court also decided that there was not enough of a link between the infringing activity and Netcom's finances to hold Netcom vicariously liable, but it did not rule on the contributory question.

Although there were other cases after *Netcom* where ISPs were held liable,[12] an important precedent had been set. It became understood that any interceding service that did not upload infringing content directly should not be held directly responsible for the illegal and/or infringing actions of its customers.

It was not long until this principle was set into law. Firstly, the Berne Copyright Convention allows member states to set exceptions and limitations to the

---

[7] *Playboy Enterprises, Inc. v Frena*, 839 F. Supp. 1552 (M.D.Fla. 1993).

[8] *Sega Enterprises v Sabella*, No. C93-04260 (N.D. Cal. 1996).

[9] *Sega Enterprises Ltd. v MAPHIA*, 857 F. Supp. 679 (N.D. Cal. 1994).

[10] The cases are: *Adobe Systems Inc. v Community ConneXion Inc.*, No. 96-20833 (N.D. Cal., filed 10/8/96); and *AdobeSystems Inc. v Tripod Inc.*, No. 1:96CV157 (N.D. W.Va.).

[11] *Religious Technology Center v Netcom Online Communication Services, Inc.*, 907 F.Supp. 1361 (N.D. Cal. 1995).

[12] For example, *Geffen Records, Inc., et al. v Arizona Bizness, et al.*, No. 98-CV-00794, (D. Ariz. 5/5/98), where representatives of the music industry won a temporary restraining order against an ISP that allowed illegal MP3 music downloads.

exclusive right of reproduction that comply with the three-step test[13] contained in Art. 9(2), which states that limitations must be "in certain special cases, provided that such reproduction does not conflict with a normal exploitation of the work and does not unreasonably prejudice the legitimate interests of the author." The World Intellectual Property (WIPO) expanded the application of the three-step test to all other rights protected by the 1996 WIPO Copyright Treaty (WCT).

The existence (and expansion) of the three-step test allowed the enactment of the introduction of a very strong limitation of liability contained in the DMCA in the United States. §512 of the DMCA[14] dictates that intermediaries shall not be held liable for monetary or injunctive relief for content uploaded to a network by its users if they do not have actual knowledge that the material uploaded to their systems is infringing; and that when it is notified of the presence of such items, "acts expeditiously to remove, or disable access to, the material".

This limitation was eventually replicated throughout Europe with the enactment of the E-Commerce Directive.[15] In the prelude of the instrument, the EU states clearly that this is an area where harmonisation is necessary for the proper functioning of the common market, as it would create barriers to the cross-border provision of services, and lead to competitive distortions. The EU recognised that there is a balance to be struck, and created a system of exemption of liability for intermediaries who act as "mere conduit" and do not exercise an editing or monitoring function. The Directive establishes that an intermediary that expeditiously removes access to illicit content once notified will therefore not be held liable for that content. Art 12.1 states that a service provider will not be liable for the information transmitted via its network if it does not initiate the transmission; does not select the receiver of the transmission, and does not modify its content.

Moreover, the E-Commerce Directive ruled out the creation of monitoring obligations for intermediaries. Art. 15 says that the limitation of liability should not be read as providing any obligation "to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity." In other words, providers of online services will not be responsible for illegal content that has been made available in their networks by customers if they are mere conduits and also have procedures in place to remove the content quickly, and they will not be obliged to monitor activity in advance.

The principle of limitation of liability for ISPs and other middle-men has spread to many other jurisdictions. For example, the multilateral trade agreement between the United States and Central American countries, known as the Dominican Republic-Central American Free Trade Agreement (DR-CAFTA)

---

[13] Senftleben MRF, *Copyright, Limitations, and the Three-Step Test: An Analysis of the Three-Step Test in International and EC Copyright Law*, The Hague; London: Kluwer Law International (2004).

[14] §512(c)(1), Title 17, Chapter 5, U.S. Code.

[15] 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, OJ L 178/1 (2000).

contains requirements for intermediary liability for copyright infringement in Article 15.11.27, and is closely modelled on US DMCA's liability provisions.[16]

Given the international prevalence of this principle, our discussion should end right here, at least for those countries that have enacted limits for responsibility for illegal content. The law is very clear, there are safeguards for content owners, and there appear to be very little room for interpretation, with the exception of some border cases, and perhaps to try to delimit some of the concepts a bit more. But unfortunately (or fortunately, depending on your point of view), the legislation described above has not stopped the debate. For some years now, regulators and industry have been trying to re-open the question of liability.

This has been some time coming. After intermediaries were given an almost blank cheque to operate with immunity, interested parties tried to find other ways to curb illicit practices online, particularly Internet piracy. This led to a series of attempts to destroy the makers of software that made it possible to exchange files, a strategy that had varying levels of success in the courts,[17] but which failed to stop online copyright infringement. Then there were several misguided and eventually failed attempts to pursue customers directly through litigation,[18] but needless to say, an industry that decides that its only avenue for survival is to sue its own consumers is not going to reap much sympathy, and such strategies tend to backfires. Throughout this time, the consensus remained that in general it would be difficult for any Internet service provider to monitor and filter every transaction performed by their customers, and therefore the respect for limitation of liability held.

Fast-forward some years, and the picture changed immensely. In the early days of the Internet, intermediaries used to be small and medium operations that did not have enough money to pay back in case of litigation. But with the appearance of large aggregated services such as Google, the possibility of making these providers liable became greater. The cluster of lawsuits against Google that we have witnessed in the last few years has been the result of this change in strategy. However, service providers are still protected by safe harbours and other liability dampeners.

---

[16] Brown A, Guadamuz A, and Hatcher J, "The Impact of Free Trade Agreements on Information Technology Based Business", 2:1 *Geopolitics, History, and International Relations* 62 (2010).

[17] See US cases such as *A&M Records v Napster*, 2002 U.S. App. LEXIS 4752; *In re Aimster Copyright Litig.*, 2004 U.S. App. LEXIS 1449; *Metro-Goldwyn-Mayer Studios Inc. v Grokster, Ltd.*, 125 S. Ct. 2764; and the Australian case *Universal Music Australia v Sharman License Holdings* [2005] FCA 1242.

[18] Hughes J, "On the Logic of Suing One's Customers and the Dilemma of Infringement-Based Business Models", 22 *Cardozo Arts & Entertainment Law Journal* 725 (2005).

3. If at first you fail, try and try again

3.1 L'Oreal

Given the clarity of the law, it may seem surprising that there would still be anyone intent on collecting money from intermediaries. But this is precisely what took place in many jurisdictions.

One of the most important European cases dealing with the question has nothing to do with copyright, but rather trade mark; it is the European Court of Justice case of *L'Oréal v eBay.*[19] The case was brought by cosmetic manufacturer L'Oreal against the large auctions website eBay for the actions of distributors of unauthorised sampler products, who removed the sampler package and then sold the products on the site. The question at the heart of the case was whether eBay can be held liable for trade mark infringement committed by merchants operating in its website. A simple reading of the aforementioned Electronic Commerce Directive would indicate that they are not, but the facts of the case complicated the issue somewhat. While it seems like eBay is not to be held liable for whatever is sold on its site by third parties, eBay allowed the placement of sponsored links to infringing products. It also included the unauthorised merchants to include listings under the affected marks, in other words, if you looked under L'Oreal you would find both authorised and unauthorised distributors. Moreover, infringing merchants could purchase Google Adwords and other keyword search engine placement that directed to the pages on eBay. The question then was whether these actions warranted liability.

The High Court of England decided the case at an earlier stage in 2009.[20] Arnold J found that there had been indeed trade mark infringement committed by some of the co-defendants by trading on sampler and de-marked goods on the site. He also ruled that eBay was not jointly liable for infringement, which was consistent with the prevalent principle of limitation of intermediary liability. However, Arnold J referred some important questions to the ECJ, some of which dealt with specifics of trade mark law and with injunctions.

The relevant question regarding intermediary liability asked shether eBay Europe had a defence under Art. 14 of the E-Commerce Directive. Article 14 of the E-Commerce Directive gives a specific defence regarding hosting, which states that an information service provider that provides "storage of information provided by a recipient of the service" will not be held liable if the provider does not have knowledge of the illegal activity, and upon being made aware of the existence of any illicit content in its storage facilities, it removes it promptly, or disables access to it.

The ECJ produced an interesting ruling that both maintains the principles of intermediary liability, but finds that some of eBay's actions to fall outside of the general protection. Dealing with the issue of intermediary liability, the ECJ declared that the Art 14(1) of the E-Commerce Directive must be interpreted as applying to the operator of an online marketplace if they have not had

---

[19] *L'Oréal SA and Others v eBay International AG and Others* C-324/09.

[20] *L'Oreal SA & Ors v EBay International AG & Ors* [2009] EWHC 1094.

knowledge or control over the data stored on its site. However, if the operator plays a role that provides assistance, then it might not be covered by the exemption from liability "if it was aware of facts or circumstances on the basis of which a diligent economic operator should have realised that the offers for sale in question were unlawful", and also failed to act expeditiously to remove the content.

This is a very interesting test. If an Internet intermediary plays an active role in assisting people to optimise the presentation of an infringing product, then they might be held liable. However, even if the intermediary did not play any active role in presenting the goods, they might still be held liable if they could have known that the goods offered were unlawful. Unfortunately, there seems to be no determination as to volume of transactions, so it might be difficult for an operator to be able to know the legality of an item when it handles millions of transactions per day.

The truth is that the *L'Oreal* case has given us a reasonable test for liability, but also has set the boundaries of the actions that an intermediary has to perform in order to be held responsible for content posted by its users.

3.1 iiNet

To contrast what is happening in Europe and the US, we have to look at a country that does not have the same level of limits placed on legal accountability of service providers. Australia does not have in place any regime that mirrors the DMCA's safe harbours, or the EU's E-Commerce Directive. According to Australian commentators, the type of defences and safe harbours available under its Copyright Act are extremely limited, tremendously complicated, and mostly inadequate to ensure that access providers can successfully conduct their business without fear of being sued for copyright infringement.[21]

Australian courts were asked to test intermediary liability in the landmark case of *Roadshow v iiNet*.[22] iiNet is an Australian internet service provider that was sued in 2008 for authorisation[23] of copyright infringement by Australian film producer Roadshow Films and a conglomerate of international film producers including Warner, Columbia, 20th Century, and Sony Pictures. The question at the heart of the proceeding is typical of the many cases described above, and it was whether an ISP is to be held liable for the copyright infringement committed by its customers. The case was decided in first instance in 2010, and then the plaintiffs appealed to the Australian Federal Court, which denied the appeal in 2010.

At first glance the case might seem to lack relevance to an international analysis of intermediary liability because, as it has been mentioned, Australia has little

---

[21] Weatherall K, *Internet Intermediaries and Copyright: An Australian Agenda for Reform*. Policy Paper for the Australian Digital Alliance (2011), http://bit.ly/140eh0b.

[22] *Roadshow Films Pty Limited v iiNet Limited* [2011] FCAFC 23.

[23] The Australian figure is a type of secondary liability for sanction, approval and countenance of an infringing act. See: Napthali M, "Unauthorised: Some thoughts upon the doctrine of authorisation of copyright infringement in the peer-to-peer age", 16 Australian Intellectual Property Journal 5 (2005).

limitation of responsibility for ISPs. Similarly, the case is unique because Australian copyright law holds secondary infringement as direct infringement. In other words, anyone making available copyright works will be held similarly liable, whether they do so directly or indirectly. Nonetheless, iiNet is interesting precisely because it shows what the legal landscape may look like without existing safe harbours. It is also quite an illustrating case from a technical and legal standpoint because it contains some detailed legal analysis of file-sharing technologies.

In the first instance[24] Cowdroy J explores several issues, but accurately identifies that the case hinges on two simple questions. Have the iiNet customers infringed copyright directly? The answer is unequivocally yes. Has iiNet authorised the copyright infringement of its users by failing to take steps to stop it from happening? Here the answer is no. The judge considers that there is a very clear distinction between an ISP, which "simply cannot be seen as sanctioning, approving or countenancing copyright infringement",[25] and the producer of software designed specifically to authorise copyright infringement, such as P2P software manufacturers like Kazaa and Napster. Based on this, the judge found that iiNet had not authorised copyright infringement, and therefore was not liable. Interestingly enough, the judge was asked to explore whether iiNet fell under the protection of the limited safe harbour provisions present in Australian copyright law,[26] and found that they would indeed satisfy those requirements, but that they did not need such protection because there was no authorisation, in other words, there was no secondary liability.

The film studios appealed the decision, which was denied by the Federal Court, although their reasoning was different. As with the ruling in first instance, the matter came precisely to the question of whether or not iiNet had authorised copyright infringement committed by its customers. The Federal Court concluded that there is no authorisation, but commented:

> *"However, while the evidence supports a conclusion that iiNet demonstrated a dismissive and, indeed, contumelious, attitude to the complaints of infringement by the use of its services, its conduct did not amount to authorisation of the primary acts of infringement on the part of iiNet users."*[27]

The court found that content owners would have to meet a high threshold level of infringement in similar cases in the future, although the court left open the possibility of similar litigation as every situation will have to be analysed as to whether the court has done enough to prevent infringement.

Despite the above cases, limitation of liability for intermediaries has remained the norm in most jurisdictions where it has been implemented, and with a few

---

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

[25] Ibid, para 14.

[26] Included in Division 2AA of Part V of the Copyright Act 1968.

[27] FCAFC appeal, at para 257.

exceptions,[28] service providers have managed to remain relatively free to operate without fears of overwhelming litigation. Content owners then have had to pursue other strategies.

4. Blocking and filtering

4.1 European cases

Given the limitations in place that favour ISPs and other mediators, some elements of the copyright industry tried to find other ways that would allow them to target intermediaries, but in ways that would not fall foul of the existing rules. One of the ways of doing this would be to target ISPs with injunctions, but not to remove content as such, but to try to implement the filtering and blocking of infringing materials with the intention of impeding it from ever reaching customers.

This follows a type of Internet regulation that has been called control of the chokepoints [29] This idea is behind some of the most successful (and controversial) regulatory solutions of the last decade, which includes the Great Firewall in China,[30] and the Internet Watch Foundation (IWF)[31] in the UK. While the efficiency of filtering and blocking is still under discussion, there seems to be little doubt that, at least to a certain extent, some amount of filtering can indeed avoid content from reaching some target audiences. The IWF for example deals specifically with the blocking in the UK of child pornography by the identification of URLs that lead to illegal content. This creates a list that is sent to ISPs, who voluntarily block access to those sites.[32]

Getting repressive countries to filter content, and getting ISPs to make efforts to block child pornography is one thing. Can the copyright industry manage to make ISPs into content filters?

This possibility was explored at length in the long-running ECJ case of *Scarlet v SABAM*.[33] The Belgian Society of Authors, Composers, and Publishers (SABAM) initiated the case in 2004 against service provider Tiscali (which later changed its name to Scarlet). SABAM alleged Tiscali's users were illegally downloading works in its catalogue from the Internet via P2P networks, and wanted Tiscali to

---

[28] See for example a recent case in an Amsterdam court where a USENET intermediary received an injunction to remove content posted by users. See: Crinjs K, "Dutch BREIN wins lawsuit against major European Usenet Provider", *Future of Copyright* (October 1st, 2011), http://bit.ly/12q4lzV.

[29] Goldsmith JL and Wu T, *Who Controls the Internet? Illusions of a Borderless World*, Oxford: Oxford University Press (2006).

[30] Stevenson C, "Breaching the Great Firewall: China's Internet Censorship and the Quest for Freedom of Expression in a Connected World" 30 *Boston College International and Comparative Law Review* 531 (2007).

[31] Laidlaw E, "The Responsibilities of Free Speech Regulators: An Analysis of the Internet Watch Foundation" 20 *International Journal of Law and Information Technology* 312 (2012).

[32] Edwards L, "From Child Porn to China, In One Cleanfeed", 3:3 *SCRIPTed* 174 (2006).

[33] *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* C-70/10.

install filtering software in its network that would curb further infringement. The first ruling in the District Court of Brussels agreed with the claimants based entirely on expert reports about the feasibility of deploying filtering systems. The expert argued that there were at least thirteen systems capable of effectively filtering P2P transmissions, seven of which could be deployed in Tiscali's servers. Tiscali's response was that these solutions were partial and ineffective at best, as P2P clients are increasingly becoming more difficult to filter because of encryption technology.

Unsurprisingly, the decision was appealed. The Brussels Court of Appeals rightly realised that this went beyond the limitation of liability contained in the E-Commerce Directive, and there was a chance that there might be a conflict between the Copyright Directive 2001/29,[34] the IP Enforcement Directive 2004/48,[35] the Data Protection Directive 95/46,[36] the Electronic Privacy Directive 2002/58,[37] and Articles 8 and 10 of the European Convention on Human Rights (ECHR). The referring court sought guidance on whether it would be possible for a national court to order putting in place by injunction a widespread and indiscriminate filtering system which would require constant monitoring at the expense of the ISP, as it might violate fundamental rights and freedoms enshrined in various directives and conventions, and if so, if such relief would have to respect principles of proportionality. The Belgian court was clearly troubled by the implications of enacting such a system without a substantive ruling, and that copyright owners would be able to impose great costs to ISPs simply by asking it via injunctive relief.

The ECJ answered that indeed a copyright filtering injunction would create a clash with other legal principles. It became clear from the start that the ECJ was not amenable to rule in favour of indiscriminate monitoring, as it would go against Art. 15 of the E-Commerce Directive, which, as has been mentioned, states unequivocally that Member States shall not require intermediaries to monitor the information which they transmit or store. Any filtering system would be in violation of this rule, as it would require the following acts from the ISP:

> *"– first, that the ISP identify, within all of the electronic communications of all its customers, the files relating to peer-to-peer traffic; – secondly, that it identify, within that traffic, the files containing works in respect of which holders of intellectual-property rights claim to hold rights;*

---

[34] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society OJ L 167/10 (2001).

[35] Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights OJ L 157/16 (2004).

[36] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281/31 (1995).

[37] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector OJ L 201/37 (2002).

– thirdly, that it determine which of those files are being shared unlawfully; and
– fourthly, that it block file sharing that it considers to be unlawful."

Moreover, the court stated that rights protected under intellectual property legislation are indeed enshrined in the Charter of Fundamental Rights of the European Union, but that these rights are not absolute, and must be read in conjunction with other legislation. Specifically citing the *Promusicae* case,[38] the court commented that the protection of IP rights "must be balanced against the protection of other fundamental rights", and that "in the context of measures adopted to protect copyright holders, national authorities and courts must strike a fair balance between the protection of copyright and the protection of the fundamental rights of individuals who are affected by such measures."

The ECJ then considered that there are fundamental rights that would be affected by the filtering system proposed by SABAM, namely the freedom to conduct business by the ISPs because the system would be costly, and that the intermediaries would solely foot this cost. To support this view, they stated that Art. 3 of the IP Enforcement Directive requires that IP remedies "shall be fair and equitable and shall not be unnecessarily complicated or costly, or entail unreasonable time-limits or unwarranted delays". For users, the filtering system would affect their "right to protection of their personal data and their freedom to receive or impart information", protected by Arts. 8 and 11 of the ECHR.

Finally, the ECJ opined that there were some serious procedural problems with a system that would be enacted by injunction for works that were not even created at the time that the injunction was issued. Nonetheless, specific injunctions are still allowed, what the ECJ ruled against was a blanket filtering system suggested by SABAM. The court created a checklist for similar future blocking requests:

"[The cited Directives] read together and construed in the light of the requirements stemming from the protection of the applicable fundamental rights, must be interpreted as precluding an injunction made against an internet service provider which requires it to install a system for filtering

- *all electronic communications passing via its services, in particular those involving the use of peer-to-peer software;*
- *which applies indiscriminately to all its customers; as a preventive measure;*
- *exclusively at its expense; and*
- *for an unlimited period,*

which is capable of identifying on that provider's network the movement of electronic files containing a musical, cinematographic or audio-visual work in respect of which the applicant claims to hold intellectual-property rights, with a view to blocking the transfer of files the sharing of which infringes copyright."

This is a reasonable and interesting ruling that handles most of the balancing aspects of copyright enforcement, and sets the boundaries of what filtering should look like in the future. The ECJ reached a very similar solution in the case

[38] *Productores de Música de España (Promusicae) v Telefónica de España SAU* C-275/06.

of *SABAM v Netlog*,[39] in a situation that closely mirrored the one covered in *Scarlet*. Here, the Belgian collecting society sued a social network site named Netlog, attempting to obtain an injunction ordering it to install filtering software in its network. The site fought the injunction, and much as its predecessor case, it made it all the way to the ECJ, where the court followed its preceding reasoning closely, finding that indiscriminate filtering systems are contrary to the dispositions contained in the E-Commerce Directive, and are also disproportionate.

4.2 Blocking orders

It might be surprising that given the high-threshold test of the ECJ's SABAM cases, several courts around Europe have been actually enforcing filtering against specific sites. Just to give one example, the popular tracker site The Pirate Bay has now been blocked in one way or another in at least 12 countries in Europe, including Italy, Sweden and Denmark.[40] It seems that the long-term effect of SABAM is to allow targeted block orders against specific sites, a strategy that is perhaps not what content owners sought after, but that allows for a limited number of victories in the courts against specific sites.

One of the most interesting developments has taken place in the UK, where copyright holders have successfully led a blocking campaign against various torrent-tracking sites.

The story began with the case of *Twentieth Century Fox & Others v Newzbin.*[41] The case originated when several Hollywood film studios sued Newzbin, a then popular filesharing site, for copyright infringement by communicating to the public.[42] Newzbin operated a subscription service that encouraged its users to share all manners of content, and therefore the court found it quite easy to get a ruling that the site's operators were liable directly for copyright infringement. During the trial, the defendants tried to argue that they were a service provider and therefore were not liable for copyright infringement committed by its customers. The judge disagreed, as it was evident that the owners had specific knowledge of the infringement that was taking place on the site.

With a solid copyright infringement result in hand, the plaintiffs sought to obtain an order to get British Telecommunications (BT) to filter content from Newzbin, and the High Court of England and Wales acquiesced by instating a court-mandated system of Internet filtering against Newzbin.[43] The studios sought this order as they argued that it was the only way in which they would be able to implement the substantive ruling. The High Court agreed with the studios, and

---

[39] *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV* C–360/10.

[40] See for example, *Bergamo Public Prosecutor's Officer v Kolmisappi* (Italian Supreme Court of Cassation, 29 Sept 2009); *Columbia Pictures Industries Inc v Portlane AB* (Swedish Court of Appeal, 4 May 2010); and *IFPI Danmark v DMT2 A/S* (Frederiksberg Court, 29 October 2008).

[41] *Twentieth Century Fox Film Corporation & Anor v Newzbin Ltd* [2010] EWHC 608.

[42] Contemplated in s20 of the Copyright, Designs and Patents Act 1988.

[43] *Twentieth Century Fox Film Corp & Ors v British Telecommunications Plc* [2011] EWHC 1981.

BT was forced to technically block access from its customers to the Newzbin website. Kitchin J ruled that he accepted the suggested order from the studios.

The reasoning used to issue the blocking order relies heavily on technical grounds. The High Court took into consideration the existence of a voluntary service such as the IWF as evidence that the blocking of IP addresses is possible. This line of argument follows that if it is possible to restrict access to child pornography, then it is also possible to do the same for some copyright infringing sites like Newzbin.

Unfortunately, the court really failed to properly address the efficiency of filtering and blocking orders, which should have played a much stronger part of any legal ruling dealing with this subject. If the objective of the plaintiffs is to block access from UK customers to a specific infringing site, having this judicial order is not going to help, there are several ways in which the order can be easily circumvented. The movie studios and the Court seemed to know this, but they went ahead nonetheless, as there are strong hints that the ruling has the ultimate objective of providing an example to others. The Court seems uninterested in the efficiency of the order, what is important is that a message is sent to other operators and potential infringers.

Interestingly, the Newzbin ruling came before SABAM case had been decided, and therefore the Court only had a translation of the opinion of the Advocate General to go by before the court had made its decision. This might be the reason why the actual legal content of the case tends to ignore the considerations contained in SABAM that have already been explained above, and issued the blocking order regardless.

The result of the Newzbin case was massive, as it opened the floodgates for other similar blocking orders. The next site in line was The Pirate Bay (TPB), the golden goose of torrent tracker providers.

Given the precedents, it is unsurprising that the High Court ruled that UK Internet service providers must take steps to technically block access from their customers to The Pirate Bay.[44] Several recording companies and representatives of the music industry filed a suit against a number of ISPs to try to obtain a blocking injunction similar to the one obtained in *Newzbin*. There is a slight difference with what happened in that other case, as the music industry did not file a claim directly against TPB, but rather did it against the intermediaries without joining the defendants. The Court had to consider the infringement aspect of the case separately[45] before issuing the blocking order.

There is very little meat in the actual wording of the decision. This is because most of the legal framework that sustains the order was undertaken in previous cases, namely in blocking access to Newzbin; and to a lesser extent in other similar cases such as *Golden Eye v Telefónica*.[46] The misapplication, and perhaps even complete bypassing of the two ECJ SABAM cases is baffling, with Newzbin

---

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

[45] *Dramatico Entertainment Ltd & Ors v British Sky Broadcasting Ltd & Ors* [2012] EWHC 268 (Ch).

[46] *Golden Eye (International) Ltd & Anor v Telefonica UK Ltd* [2012] EWHC 723 (Ch).

there was reason as it precedes the first SABAM case, but with The Pirate Bay block, there really was no reason to ignore it. Talking about SABAM, and the conflicts of values with the human rights and the principle of proportionality, Arnold J opined that it had read the reasoning presented in both cases, and considered that it did not call into question the reasoning in Newzbin. This is a quick and disappointing dismissal of SABAM, which undoubtedly offers a detailed step-by-step test for future blocking orders. The problem is that both Newzbin and TPB orders ignore the balancing act displayed by the ECJ in SABAM, not only with regards to cost, but also when it considered human rights and data protection. The judge here displays a disregard for those arguments.

Moreover, the legal issue in the TPB case rests on the question of whether a court has the power to order intermediaries to exercise technical blocking of specific websites where copyright infringement is taking place. As this question had already been answered positively in Newzbin, all that is required is for a judge to be convinced that a site is being used mostly for copyright infringement, and an order to block it can be issued.

As it was pointed out above, TPB were not an actual party of the proceedings, there was surprisingly little consideration given to the matter of copyright infringement committed by The Pirate Bay and its customers. The reason for this is that the defendants in this case were several UK ISPs, and as such, they were really not interested in defending TPB. Arnold J seems content to simply state that TPB (and its users) infringe copyright given the evidence of the fact presented by the music industry. Therefore, there was no need to serve TPB with a notice because even the courts in Sweden were unable to reach them.

Just as with Newzbin, the ruling relies heavily on the technical aspects of the order. Here Arnold J seems content once more to take the claims of the copyright holders and to gloss over the fact that the order will be easily circumvented. It is true that copyright enforcement mechanisms allow for the implementation of injunctions and court orders that will try to prevent further infringement from taking place. Blocking access to an infringing site is the logical next step in the legal fight against piracy. The problem that these orders are not very efficient is ignored. Presented with a block, those knowledgeable enough will simply bypass it.

Despite these misgivings, it would appear that blocking orders are here to stay. In *EMI Records v B Sky B*,[47] the High Court of England and Wales produced a third high-profile blocking order for UK ISPs against three popular torrent sites called KAT, H33T, and Fenopy. Just as with TPB, the action was brought by the music industry directly against the intermediaries and not against the site owners.

The case is quite straightforward, as it follows closely the format established in Newzbin and The Pirate Bay. The ruling briefly discusses that the orders are deemed proportional given the seriousness of the offence, and declares that the court has jurisdiction over the case. Just like the decision against TPB, in this instance Arnold J goes into the substantive issue of whether there is copyright infringement taking place. One of the interesting parts of this ruling is that it

[47] *EMI Records Ltd & Ors v British Sky Broadcasting Ltd & Ors* [2013] EWHC 379 (Ch).

clearly distinguishes the copyright liability of the users, and that of the operators of the tracker sites.

In first instance, Arnold J examined that the users of the site are engaged in both direct copyright infringement, and also in communication to the public. This is hardly surprising, but as the copyright industry has been moving away from suing users, this fact is kept only as evidence that there is indeed copyright infringement going on in those sites. With regards to the operators for KAT, H33T and Fenopy, the claimants argued that they were liable for copyright infringement for three reasons. Firstly, the sites are indeed communicating protected works to the public, which makes them guilty of copyright infringement. Secondly, the ruling finds that the operators are guilty of the tort of authorising infringement, so the sites are jointly liable for infringement committed by their users. Thirdly, the operators of the sites have actual knowledge of the infringement, and base their business model on piracy. This weighs heavily on the issuing of blocking orders.

All of the above is to be expected as it follows closely the line of reasoning that started with Newzbin. However, what makes this case particularly important for the purpose of this discussion is that it goes into a further analysis of the efficiency of blocking orders, which is something that was definitely missing from the previous decisions. Arnold J makes a very interesting statement in that regard. He claims that the effect of the Italian blocking order resulted in a 73% reduction in audience going to The Pirate Bay, and an astounding 96% reduction in page views. He also claimed that before the TPB blocking the site was ranked 43 in the web-metric site Alexa for the UK, while after the block it had fallen to number 293.

These are some remarkable claims. If taken at face value, they would prove to be unequivocal evidence that blocking orders do work really well, and that the result is a clear reduction in traffic against blocked sites.

However, extraordinary claims require extraordinary evidence, and I have not been able to find any corroboration to these factual statements contained in the ruling. On the contrary, a report by the UK's OFCOM[48] looking at the efficiency of blocking orders specifically stated that these are not particularly efficient as people who are willing to do so can easily circumvent them. Furthermore, the report concluded that:

> *"To be successful, any process also needs to acknowledge and seek to address concerns from citizens and legitimate users, for example that site blocking could ultimately have an adverse impact on privacy and freedom of expression.*
> *Any process designed to generate a blocking injunction also needs to be fair, such that the legitimate interests of other interested parties (i.e. sites which could be blocked by these processes, the end users who may lose access to particular content and the ISPs who may be involved in blocking obligations) can be properly considered by a Court."*

[48] OFCOM. *"Site Blocking" to Reduce Online Copyright Infringement: A Review of Sections 17 and 18 of the Digital Economy Act*. Official Advice, (2010), http://bit.ly/175vMBN.

This is largely what was concluded by the ECJ in SABAM, and it is precisely the type of analysis that is lacking in the three cases under analysis.

Moreover, the problem with the statistics cited by the judge is precisely that it is extremely difficult to obtain data about a block because those who are intent on circumventing the order will not be easy to track. For example, if people in Italy are using a proxy server[49] or a virtual private network (VPN)[50] to bypass the TPB blocking, it is obvious that they will not show up in normal metrics as accessing the site from Italy at all.

Similarly, the claim that one can gather any meaningful data from Alexa rankings is highly suspect. Alexa works by measuring the behaviour of users who have installed a toolbar in their browser. This gives a snapshot of a very narrow demographic, that of Alexa toolbar users. Needless to say, people who are more likely to share files online are less likely to have any sort of toolbar installed on their browsers, particularly one that tracks online behaviour. Similarly, there are studies[51] that prove that Alexa's rankings tend to be wrong for both small and big websites, as they produce some serious mismatches with reality.

In the end, the best way to try to ascertain the effect of ISP blocking orders is to ask the people who are engaged in the practice. This is precisely what was done by Dutch researchers,[52] which conducted a survey of thousands of users about their downloading behaviour. While more than 75% of respondents claimed that they never downloaded any illegal content, those who engaged in the practice replied that they were not affected whatsoever by the blocking of TPB in the Netherlands. Only 3.6% claimed that they are downloading less, and only 1.9% admitted that they had stopped downloading entirely. This seems like a huge failure for blocking orders.

Despite the evidence, the growing number of cases allowing blocking injunctions is undoubtedly going to continue. Similarly, legislators are following suit and giving a stamp of approval to this approach. The UK government passed the Digital Economy Act 2010, which contains a section specially dedicated to secure blocking injunctions.

We can conclude that while the evidence continues to point towards the lack of efficacy of blocking and filtering efforts, legislators, content owners and the courts will continue to use them, because at least it allows them to believe that something is being done to stop online piracy.

---

[49] These are sites that allow users to mask their originating IP address, making it possible to circumvent blocks.

[50] These are encrypted private networks that make it look as if the user is browsing the Internet from another country, which also can bypass filters.

[51] Arrington M, "Alexa's Make Believe Internet", *TechCrunch* (November 25, 2007), http://tcrn.ch/166ldu0.

[52] Poort J and Leenheer J, *Filesharing 2©12, Downloaden in Nederland*, Institute for Information Law (IViR) Report (2012), http://bit.ly/166lWv7.

5. Graduated response

If this paper had been written a few years earlier, then it would have dealt mostly with the growing trend towards graduated response, also known as three-strikes legislation. This is because several countries started playing with the idea of turning Internet service providers into copyright enforcers.

The idea behind graduated response is that content owners would identify habitual file-sharers through their IP address, and then they would send a notice to the ISP that owns such an address. After this step, there are various different manners in which the intermediary would have to comply, the most common of which would be for the provider to send a letter of warning, followed by a second warning, and then if the infringement continued there would be a disconnection order (hence the nickname "three strikes").[53]

France has been the most prominent example of the graduated response with the passing in 2009 of the *Loi favorisant la diffusion et la protection de la création sur internet*,[54] which established a governmental authority called the *Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet* (HADOPI), which is also the name by which the law is better known. The legislation allows a copyright holder to send a complaint to HADOPI detailing the nature of the offence and the IP address involved. The authority may then initiate a process by contacting the ISP in question. The provider sends a notice to the account-holder of the offending IP address, initiates a monitoring of the account, and might impose filters. If there is a repeat offence, then a second notice will be sent. If after a year after the second notice there is a continuation of the offender, then the ISP is required to suspend the Internet connection, the user is blacklisted, and other ISPs are notified.

Many other countries adopted similar type of legislation, including New Zealand, Korea, Taiwan, Chile, and the UK.[55] Despite this initial push, many other countries decided not to adopt three-strikes regimes, including Sweden, Germany and Spain.[56]

The largest blow to the idea that ISPs should be able to disconnect users for copyright infringement came through the "Telecomms Package",[57] which implemented an amendment (Amendment 138) tabled by the European Parliament during deliberations in 2008, that was to be included in the Framework Directive 2002/21/EC.[58] The European Parliament passed the

---

[53] Yu PK, "The Graduated Response", 62 *Florida Law Review* 1373 (2010).

[54] France, LOI n° 2009–669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet.

[55] Edwards L, *The Role and Responsibility of Internet Intermediaries in the Field of Copyright and Related Rights*. WIPO Report WIPO-ISOC/GE/11 (2011).

[56] Ibid.

[57] Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC, 2002/19/EC, and 2002/20/EC, OJ L 337/37 (2009).

[58] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services OJ L 108/33 (2002).

amendment 138 during the first two readings of the Telecomms Package, and it included the following paragraph to Art 8.4:

> *"applying the principle that no restriction may be imposed on the fundamental rights and freedoms of end-users, without a prior ruling by the judicial authorities, notably in accordance with Article 11 of the Charter of Fundamental Rights of the European Union on freedom of expression and information, save when public security is threatened in which case the ruling may be subsequent."*[59]

This clearly reads as an indictment of all graduated response, as it requires that any restriction on the rights of end-users would have to be handed-in by a court order, and not by a private administrative procedure as is necessitated by the prevailing graduated responses solutions. However, the above text came under fire by the Commission just before third reading, as it was seen as going too far. If the text had been kept like this, it would have had serious implications for existing laws like HADOPI. The institutional stand-off was diverted by the adoption of a compromise text that includes a new provision to Art 1 of the Framework Directive that reads:

> *"3a. Measures taken by Member States regarding end-users access' to, or use of, services and applications through electronic communications networks shall respect the fundamental rights and freedoms of natural persons, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and general principles of Community law.*
> *Any of these measures regarding end-users' access to, or use of, services and applications through electronic communications networks liable to restrict those fundamental rights or freedoms may only be imposed if they are appropriate, proportionate and necessary within a democratic society […]"*

This does not affect graduated response measures already deployed, but it creates the principle that any sort of restriction to access to the Internet should be performed if they are "appropriate, proportionate and necessary". This is an interesting case in which IP law is a subordinate of human rights law.

This connection between basic rights and the Internet is a growing trend, and explains the fact that more decisions about ISP liability may have to consider human rights before the rights of copyright holders, and therefore explains the decreasing viability of graduated response as a serious option for enforcement. Access to information and communication technologies is increasingly seen as a basic right,[60] and anything that might affect negatively a user's prerogatives will require a ruling by a court of law, and not just an internal ISP procedure.

An indication of the growing mandate in favour of the rights of access can be found in the resolution of the United Nations Human Rights Council on the

---

[59] See: http://bit.ly/19yyT2S.

[60] See: Guadamuz A, "Costa Rican court declares the Internet as a fundamental right", *Technollama* (October 2nd, 2010), http://bit.ly/11Y5EA4.

promotion, protection and enjoyment of human rights on the Internet.[61] This is a ground-breaking document in the history of digital rights because for the first time we have an international declaration that equates offline and online rights. The declaration is also noteworthy because it prompts governments to promote and facilitate access to the Internet. This has the effect of featuring a powerful text against legal disconnection regimes. The relevant parts of the Declaration state:

> *"3. Calls upon all States to promote and facilitate access to the Internet and international cooperation aimed at the development of media and information and communications facilities in all countries;*
> *5. Decides to continue its consideration of the promotion, protection and enjoyment of human rights, including the right to freedom of expression, on the Internet and in other technologies, as well as of how the Internet can be an important tool for development and for exercising human rights, in accordance with its programme of work."*

While this is a non-binding declaration, it can be used as an interpretation guide in future court decisions, particularly those in front of courts of human rights (eg. the Inter-American Court of Human Rights). The resolutions can also be used by the Council in case of a dispute on any abuse of human rights.

Other than the argument against disconnection from a human rights perspective, whenever one looks at graduated response one has to admit that it is a deeply flawed concept for various other reasons. The system is based on the idea that perpetrators of copyright infringement can be easily identified by an IP address, which is far from reliable. Even if an IP address is identified correctly as sharing copyright content without authorisation, and that is a big if,[62] there is still little indication about who exactly committed the offence. Particularly, in a multi-user household, there would be a serious chance of the account holder being held responsible for the actions of someone else.[63] Furthermore, the threat of disconnection could be placed towards entirely innocent people, which certainly would go against the principle of proportionality that sits at the cornerstone of the prevalent case law and legislation, at least in the EU.

Only time will tell if the trend towards dismissal of graduated response continues. There are two contrasting developments emerging at the time of writing. On the one hand, HADOPI has been under fire by a report delivered to the French Minister of Culture, which has called for a transfer of all the graduated response tasks to another department, and recommends the replacement of the disconnection third stage in favour of fines.[64] On the other

---

[61] The Human Rights Council, *The promotion, protection and enjoyment of human rights on the Internet*, A/HRC/20/L.13 (29 June, 2012).

[62] Piatek M, Kohno T, and Krishnamurthy A, "Challenges and Directions for Monitoring P2P File Sharing Networks - or - Why My Printer Received a DMCA Takedown Notice", *HotSec '08 Workshop*, San Jose California (July 28, 2008), http://bit.ly/11Y7Mb6.

[63] For an interesting case dealing with these questions, see: *Media CAT Ltd v Adams & Ors* [2011] EWPCC 10.

[64] Lescure P, *Rapport de la Mission « Acte II de l'exception culturelle » : Contribution aux politiques culturelles à l'ère numérique*. Rapport au Ministère de la Culture et de la Communication (2013), http://bit.ly/12njDj5.

hand, some ISPs in the US have signed-up voluntarily to a system called the Center for Copyright Information, which favours what is now called a "six strikes" approach by which intermediaries will send notices to users, as well as potentially reducing Internet speeds and redirecting traffic temporarily.[65] The next stage for graduated response might be an end to legislative solutions, but an increase in voluntary schemes.

6. Conclusion

At the time of writing, whistle-blower Edward Snowden has been catapulted at the top of the news by leaking information about how US intelligence services are engaging in a massive surveillance programme that accesses servers and communications from intermediary services to tap into users' data.[66] The companies involved are some of the largest technology companies in the world, including Microsoft, Yahoo, Google, Facebook, YouTube, Skype, AOL and Apple.

While the privacy and civil liberties implications of the PRISM and NSA leaks go beyond the scope of this paper, these revelations serve to emphasise the importance of intermediaries to our daily lives. It is quite indicative that intelligence agencies are mainly using existing commercial data channels, and have not had to deploy their own surveillance mechanisms. The role of the intermediary as the host and carrier of information has turned these companies into much more than mere gatekeepers, they act as information clearinghouses.

The growing important role of technological mediators is precisely why intermediary liability continues to be a relevant topic, even after all of these years. It may seem like a dry area of study, too narrow to elicit more interest than that awarded to it by IP law experts and a few technology enthusiasts. However, it is proved to be a subject that touches all sorts of interests, from security to privacy, requiring a careful balancing act.

We would therefore like to finish with a small proposal for how to regulate intermediaries. Anything that might affect users' rights has to be seen as the exception and not the norm; and any such action has to be appropriate, proportional and necessary. Nothing else will do.

---

[65] See: http://www.copyrightinformation.org/.

[66] Greenwald G and MacAskill E, "NSA Prism program taps in to user data of Apple, Google and others", *The Guardian* (7 June 2013), http://bit.ly/1939ZuD.