Northwestern Journal of Technology and Intellectual Property

Volume 11 | Issue 5 Article 4

2013

Intermediaries' Precarious Balance Within Europe: Oddly Placed Cooperative Burdens in the Online World

Anjanette H. Raymond
Indiana University, Kelley School of Business

N O R T H W E S T E R N
JOURNAL OF TECHNOLOGY
AND
INTELLECTUAL PROPERTY

Intermediaries' Precarious Balance Within Europe: Oddly Placed Cooperative Burdens in the Online World

Anjanette H. Raymond

April 2013 VOL. 11, NO. 5

Northwestern Journal of Technology and Intellectual Property
Volume 11, Number 5 (April 2013)

Intermediaries' Precarious Balance Within Europe: Oddly Placed Cooperative Burdens in the Online World

By Anjanette H. Raymond*

The Newzbin *cases mark a clear shift in the responsibility that European based internet service providers must take in protecting intellectual property rights. Previously, that burden laid primarily with rights holders. Today, however, legislative bodies and courts in both the European Union and the United States have shifted the expectation of protections to a shared burden amongst internet service providers (ISPs) and rights holders. The* SABAM *case begins to outline and define the full parameters of that shared burden. However, numerous issues exist in relation to the amount of burden each party must undertake within this shared burden standard and to date few reasonable responses have been advanced to assist ISPs in living up to this shared burden without being subjected to additional costs and potential liability. The law remains fragmented, with potential minefields abounding for ISP liability, despite the fact that service providers often work hard to comply with the law. Something must change. Namely, the entire online community—rights holders, ISPs and the online users —must share the burden of protecting intellectual property holders' rights in a way that makes sense for all parties. Placing an unsustainable burden upon ISPs will not benefit anyone and will lead to undesirable consequences.*

I. INTRODUCTION

¶1 On November 24, 2011, the European Court of Justice (ECJ) struck a blow for those who believe that ISPs should not have to monitor their users for copyright infringement. The ruling stems from the Belgian case of *Scarlet Extended v. SABAM*[1] in which an ISP provider was issued an injunction by the Brussels Court of First Instance requiring it to install filtering systems as a way to prevent copyright infringement. The company appealed the verdict and the Brussels Court of Appeals asked the European Court of Justice (ECJ) to clarify if such an injunction would be in violation of European Union laws. The ECJ ruled that requiring an ISP to perform general monitoring of consumer traffic to protect the right of intellectual property is incompatible with the E-Commerce Directive and other individual rights safeguarded by the European Union

* Assistant Professor, Department of Business Law and Ethics, Indiana University, Kelley School of Business; Visiting Fellow in International Commercial Law, Centre for Commercial Law Studies, Queen Mary, University of London. All errors, ommisions and opinions are my own. The author would like to thank Jeremy Shere and Tony Kelly for their editing and comments.

[1] Case C-70/10, Scarlet Extended SA v. Société Belge des auteurs, compositeurs et éditeurs (*SABAM*), 2011 E.C.R. I-0000. There is a second *SABAM* case, entitled *SABAM v. Netlog*, C-360/10 (16 Feb 2012). This paper will use the "SABAM" designation as a reference to the first case, Scarlet Extended [2011] ECR-I 0000.

Charter of Fundamental Rights. While the ruling might seem unremarkable since European Union law has long recognized protections for ISPs in such situations, many herald the decision as clarifying key issues at the intersection of these laws, such as the amount of burden an ISP business must undertake and the specifics in relation to the burden. However, in making its determination, the *SABAM* Court highlights but fails to resolve a growing concern for internet service providers: namely, the degree to which ISPs must bear the burden of protecting intellectual property rights.

¶2 This article will first consider the creation of the "shared burden" in the online world for the protection of intellectual property rights through an examination of the *Newzbin* cases. The article will go on to demonstrate that the *SABAM* case should be viewed as both (1) affirming the *Newzbin* court's determination of a shared burden and (2) beginning to define the parameters of service provider policing burdens in the online world. The article will next examine the *SABAM* balance in light of practical realities in the online world. Finally, the article criticizes and then suggests guidelines for the best way to protect intellectual property right holders and service providers.

II. CREATING A SYSTEM OF SHARED BURDENS TO PROTECT INTELLECTUAL PROPERTY

¶3 The United States and the European Union have long recognized the need to protect ISPs from potential liability arising from parties using their services to infringe intellectual property rights.[2] Numerous European Union directives exist along these lines, while in the United States the Digital Millennium Copyright Act[3] outlaws online

[2] While this article will primarily focus on copyright infringement in the online world, there is little doubt that numerous areas of intellectual property rights are at issue. *See, e.g.*, Myriam Davidovici-Nora, *The Dynamics of Co-Creation in the Video Game Industry: The Case of World of Warcraft*, 73 COMM. & STRAT. 43 (2009) (exploring co-creative games); Brian Holland, *Tempest in a Teapot or Tidal Wave? Cybersquatting Remedies Run Amok*, 10 J. TECH. L. & POL'Y 301 (2005) (discussing trademark and cyber-squatting); Mathias Klang, *Avatar: From Deity to Corporate Property - A Philosophical Inquiry into Digital Property in Online Games*, 7 INFO. COMM. & SOC. 389 (2004) (exploring virtual property); Lucille Ponte, *Preserving Creativity from Endless Digital Exploitation: Has the Time Come for the New Concept of Copyright Dilution*, 15 B.U. J. SCI. & TECH. L. 34 (2009) (discussing trademark and copyright dilution); Mathew Rimmer, "*Breakfast at Tiffany's:" EBay Inc., Trade Mark Law and Counterfeiting*, 21 J. L. INFO. & SCI. 128 (2011) (exploring the liability of online auction-houses for counterfeiting); Jason Schultz & Jennifer Urban, *Protecting Open Innovation: A New Approach to Patent Threats, Transaction Costs, and Tactical Disarmament*, 26 HARV. J.L. & TECH. 1 (2012) (arguing for a greater use of patent protections in the online world); Andrew Sellars, *Seized Sites: The in Rem Forfeiture of Copyright-Infringing Domain Names* (May 8, 2011), http://ssrn.com/abstract=1835604 (arguing against the use of domain name seizures); Terry Frieden, *150 Domain Names Shut Down in Probe of Counterfeit Goods*, CNN TECH (Nov. 28, 2011), http://articles.cnn.com/2011-11-28/tech/tech_websites-counterfiet-goods_1_counterfeit-goods-phony-goods-websites?_s=PM:TECH.

[3] *See generally* ORIN KERR, *A Lukewarm Defense of the Digital Millennium Copyright Act*, CATO INSTITUTE, (Adam Thierer & Warne Crews eds., 2002) (arguing for the realization that there is a logic to the organization and approaches contained within the DMCA); Bill D. Herman & Oscar H. Gandy, *Catch 1201: A Legislative History and Content Analysis of the DMCA Exemption Proceedings*, 24 CARDOZO ARTS & ENT. L.J. 121 (2006) (examining the DMCA and circumvention technology); Edward Lee, *Decoding the DMCA Safe Harbors*, 32 COLUM. J.L. & ARTS 233 (2009) (discussing the DMCA and corresponding safe harbor protections); Miquel Peguera, *When the Cached Link is the Weakest Link: Search Engine Caches under the Digital Millennium Copyright Act*, 56 J. COPYRIGHT SOC'Y U.S.A. 589 (2009) (exploring caches under the DMCA); Michael S. Sawyer, *Filters, Fair Use, and Feedback: User-Generated Content Principles and the DMCA*, 24 BERKELEY TECH. L.J. 363 (2009) (exploring user generated content liabilities under the DMCA); Philip I. Weiser & Gideon Parchomovsky, *Beyond Fair Use*, 96 CORNELL L. REV. 91 (2010) (examining fair use under the DMCA).

copyright infringement. Such laws provide protections to service providers in many common situations, such as the service provider acting as a mere conduit, caching, or hosting material, provided that the ISP does not have actual knowledge of unlawful activity.[4] However, by late 2010 it became clear that such protections were enabling service providers to entirely avoid responsibility for protecting online intellectual property rights. Thus, the time was right for a fundamental shift in understanding the practical realities of online behavior. Where previously it was believed that mainly *individuals* encouraged and perpetrated unlawful activity, it has become clear that websites can host and encourage unlawful activity, too. Given such widespread infringing activity it is not surprising that ISPs have increasingly denied access to websites hosting protected material. Yet doing so has required a shift in the location of responsibility. Previously, intellectual property rights holders were required to carry the burden of both discovery and pursuit of actions against individuals perpetrating unlawful activity. Today it seems the burden is shared, with the intellectual property rights holders required to discover illegal activity and the service provider required to enforce laws meant to prevent and stop it. This shift has not gone entirely smoothly.

¶4 The 2010 English case of *Twentieth Century Fox Film Corp. v. Newzbin Ltd.* (*Newzbin*)[5] is an example of the difficulties in protecting online intellectual property rights and the necessary shift to a shared burden. Newzbin was a content aggregator site[6] that allowed users to search the Internet for locations of a specific type of file (NZB). Similar to a torrent,[7] NZB files do not contain the file itself but rather information about the location of the file to be downloaded. A search engine is then used to locate the file or series of files and once found the file can be downloaded and viewed. The use of torrent and similar types of files has long been viewed as a clever way for a website to claim that it is not infringing copyright as the website is doing nothing more than providing links. However, similar to the peer-to-peer sharing cases of *A&M Records, Inc. v. Napster, Inc.*[8] and *MGM Studios, Inc. v. Grokster, Ltd.*[9] in the United States,[10] the

[4] *See* Council Directive 2000/31, art. 12-15, 2000 O.J. (L 178) 1 (EC) [hereinafter E-Commerce Directive].

[5] Twentieth Century Fox Film Corp. v. Newzbin Ltd. (*Newsbin*), [2010] EWHC 608 (Ch).

[6] At the most basic level, a content aggregator is a website that collects and organizes online content from other sources. It can collect information from various categories, such as news, music, videos and even books available online. RSS Readers are a good basic example.

[7] *See* Gaetano Dimita, *Six Characters in Search Infringement: Potential Liability for Creating, Downloading, and Disseminating .torrent Files*, 7 J. INTELL. PROP. L. PRAC. 466 (2012) (describing .torrent files).

[8] AM Records, Inc. v. Napster Inc., 239 F.3d 1004 (9th Cir. 2001). *See* Nick Scharf, *Napster's Long Shadow: Copyright and Peer-to-Peer Technology*, 6 J. INTELL. PROP. L. PRAC. 806 (2011) (describing the historical case).

[9] MGM Studioes, Inc. v. Grokster, Ltd., 545 U.S. 913 (2005). The *Grokster* case is frequently characterized as a re-examination of the issues in *Sony Corp. v. Universal City Studios*, 464 U.S. 417 (1984), also known as the "Betamax case." The decision in the case ultimately protected VCR manufacturers from liability for contributory infringement as the court held that technology could not be barred if it was "capable of substantial non-infringing uses." For a further discussion, see Rob Hof, *Larry Lessig: Grokster Decision Will Chill Innovation*, BLOOMBERG BUS. WEEK (June 28, 2005), http://www.businessweek.com/the_thread/techbeat/archives/2005/06/larry_lessig_gr.html (discussing the impact of the decision to the online world); Fred von Lohmann, *Remedying 'Grokster'*, LAW.COM (July 25, 2005), http://www.law.com/jsp/article.jsp?id=900005544522&Remedying_Grokster (considering the need to work around the court decision).

[10] The United States courts have previously faced an ISP issue eerily similar to the *Newzbin* and *SABAM*

film studios argued that the Newzbin site was "encouraging widespread copyright infringement by indexing unofficial copies of films."[11] The High Court in London agreed, determining that Newzbin was "liable to the claimants for infringement of their copyright,"[12] and in March, 2010, the court ordered an injunction to restrain Newzbin from infringing the "claimants' copyrights in relation to their repertoire of films."[13] Predictably, the judgment against Newzbin for copyright infringement was estimated to run into the millions of pounds. As a result, Newzbin was forced to go into administration and the website was shut down shortly thereafter. In this instance, an action against an individual and the website he operated resulted in the desired outcome, stopping widespread copyright infringement.

¶5 Not surprisingly, the *Newzbin* case did not entirely resolve the issue. In June, 2010, Newzbin came back online[14] as Newzbin2, using the same code and database as its predecessor; this time, though, the website was outside the reach of the English courts as the website was hosted outside the United Kingdom. As a result, the studios filed for an injunction in the English courts and argued that the only real means of stopping such widespread infringing activities within the United Kingdom was to seek an injunction requiring BT, a UK-based ISP, to deny access to the website Newzbin2.[15] This request is fundamental and important as it asks the English courts to recognize a shared burden of protecting intellectual property rights.

¶6 The *Newzbin2* court did not take this task lightly and carefully considered and explained legislation[16] and case law[17] within the United Kingdom and Europe. In the

cases. In the case of *Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs*, 907 F. Supp. 1361 (N.D. Cal. 1995) the Northern District of California court found that once the plaintiff had put the defendant on notice of the infringing content, the act of providing the distribution of the infringement could amount to substantial participation. In direct response to this potentially broad liability arising under the existing common law of Copyright, Congress enacted the Digital Millennium Copyright Act which specifically included a section to protect ISPs from liability provided that the ISP takes expeditious action to remove allegedly infringing content.

[11] *Newzbin*, [2010] EWHC 608 (Ch) ¶ 126.

[12] *Id.*

[13] *Id.* ¶ 135.

[14] The website page notes: "The site is no longer at this location. It now operates on a different domain name. You can use a search engine to find it." When following the advice, the website is correct: it is easy to locate via a basic Google search-top of the list. A quick glance of the landing page has the most recent episode of "The Closer" top of the list. However, it should be noted there are episodes that are not still under copyright protections. (Correct as of May 19, 2012).

[15] *See* Twentieth Century Fox Film Corp. v. British Telecomm. PLC. (*Newzbin2* (Twentieth Century Fox)), [2011] EWHC 1981 (Ch). In the United States, the DMCA is currently being used to block websites. *See* Susan Neuberger Weller, *Copyright Owners Using DMCA To Take Down URLs*, NAT'L L. R., (June 22, 2012), http://www.natlawreview.com.

[16] *See Newzbin2* (Twentieth Century Fox), [2011] EWHC 1981 ¶¶ 75-90.

[17] *See Newzbin2* (Twentieth Century Fox), [2011] EWHC 1981 ¶ 86 (citing IFPI Danmark v. Tele 2 A/S (Copenhagen City Court, 25 October 2006)) (order granted on application of the Danish branch of IFPI requiring ISP to block access to www.allofmymp3.com); SABAM v. S.A. Tiscali, Dist. Ct. Brussels No. 04/8975/A (June 29, 2007) (order granted on application of Belgian collecting society requiring ISP to filter and block infringing content); IFPI Danmark v. DMT2 A/S (Bailiff's Ct. of Frederiksberg, 5 Feb. 2008), *upheld sub nom.* Sonofon A/S v. IFPI (High Court of Eastern Denmark, 26 Nov. 2008); *sub nom.* Telenor v. IFPI (Danish Supreme Court, 27 May 2010) (order granted on application of the Danish branch of IFPI requiring ISP to block access to www.thepiratebay.org ["the Pirate Bay"]); Bergamo Pub. Prosecutor's Officer v. Kolmisappi (Italian Supreme Court of Cessation, 29 Sept. 2009) (order requiring ISPs to block access to the Pirate Bay as part of preventative seizure in criminal proceedings); Columbia Pictures Indus. Inc. v. Portlane AB (Swedish Court of Appeal, 4 May 2010) (order granted on the

United Kingdom, "the High Court shall have power to grant an injunction against a service provider, where that service provider has *actual knowledge* of another person using their service to infringe copyright."[18] In making its determination, the Court is required to take "into account all matters which appear to it in the particular circumstances to be relevant,"[19] including the service provider being given notice of the infringing activity[20] and the level of specificity of the notice.[21] Such legal proscriptions clearly place the primary burden on the rights holder to discover and then seek assistance to enforce unlawful activity. But the reality of the online environment creates a dilemma as the rights holder is sometimes faced with a single website shifting location and widely encouraging unlawful behavior, thereby making a high level of specificity unlikely in these situations. The language of the *Newzbin2* court highlights this dilemma:

> I consider that what must be shown is that the service provider has actual knowledge of one or more persons using its service to infringe copyright. The more information the service provider has about the infringing activity, the more likely it is that the service provider will have actual knowledge. Thus it may well be relevant to consider whether or to what extent the service provider has knowledge of particular copyright works (or at least classes of copyright works) being involved, of particular restricted acts (or at least types of restricted act) being committed and of particular persons (or at least groups of persons) committing those acts; but it is not essential to prove actual knowledge of a specific infringement of a specific copyright work by a specific individual.[22]

¶7 Consequently, it can be argued that while actual knowledge of infringing activity is required, there is no requirement to connect the dots and demonstrate that individual X downloaded movie Y protected by the copyright owned by movie studio Z. Instead, it could be argued that knowledge of widespread infringing activity is enough for a right holder to request an injunction. Currently, it appears that widespread infringement is considered to occur in one of two situations: (1) when numerous individuals are infringing intellectual property rights, and/or (2) when numerous incidents of infringing activity (regardless of the number of individuals) are occurring on a website. In practice,

---

application of the Studios requiring ISP to block access to a tracker website associated with the Pirate Bay); Nordic Records Norway AS v. Telenor ASA (Borgarting Court of Appeal, 9 Feb. 2010) (application for preliminary injunction by various rightholders requiring ISP to cease contributing to infringements committed through the Pirate Bay refused, Article 8(3) of the Information Society Directive not having been specifically implemented); Stichting Bescherming Rechten Entm't Industrie Nederland (BREIN) v. Ziggo BV (District Court of the Hague, 19 July 2010) (interim injunction to block access to the Pirate Bay refused); EMI Records v. UPC Commc'sn Ireland Ltd. (High Court Case No. 2009/5472P, Unreported decision of Mr. Justice Charlton, 11 Oct. 2010) (application by rightholders against ISP for blocking injunction refused since no equivalent of section 97A CDPA 1988 implementing Article 8(3) of the Information Society Directive); Constantin Film v. UPC (Commercial Court of Austria, 13 May 2011) (order granted on application of two film companies requiring ISP to block www.kino.te using IP blocking).

[18] The Information Society Directive was transposed into United Kingdom domestic law by the Copyright and Related Rights Regulations 2003, SI 2003/2498 (2003).

[19] *Newzbin2* (Twentieth Century Fox), [2011] EWHC 1981 ¶ 86 (citing Copyright and Related Rights Regulations 2003, Section 97A and 191JA).

[20] *See* 2003 Regulations, 97A 2(a) and 191J1 2(a).

[21] *See id.* at 97A 2(b) and 191J1 2(b).

[22] *Newzbin2* (Twentieth Century Fox), [2011] EWHC 1981 ¶ 148.

this means that a rights holder could discover a website with a high level of ongoing infringement even without a high level of specificity in relation to the identity of the individual or the identification of the files being illegally downloaded. Apparently, the sheer volume of illegal activity, and not the level of specificity, matters in the case of widespread infringement.[23]

¶8 This was a critical juncture. Once the court recognized that the level of actual knowledge relates only to widespread infringement on a specific website, the court is faced with a reality of online activity: that service providers are currently in the best position to assist in preventing copyright infringement.[24] This fundamental shift has occurred for two reasons. First, intellectual property holders' rights were being infringed on a "massive scale"[25] and offending websites could easily relocate. Second, the current legal standard made it almost impossible for rights holders to protect their rights in the face of wide-scale infringement as websites and relevant information were difficult to discover in a quickly changing digital landscape. Hence the court recognized that the standard simply had to be lowered. As a result, the *Newzbin2* (2011) court followed the logic and statements originating in the Information Directive,[26] that service providers are well-placed to help in such situations. Consequently, the court determined that service providers must "take measures which contribute to . . . preventing further infringements of that kind."[27] In this instance, High Court of England and Wales determined that Internet service providers can assist in the prevention of further infringement activities by blocking its United Kingdom customers' access to the website Newzbin2.[28]

---

[23] The original *Newzbin* (2010) case, in which the court was also asked to shut down the website, focused on the uncertainty arising from the large amount of "unknowns": "[I] do not believe it would be appropriate to grant an injunction of the breadth sought by the claimants for a number of reasons. First, it is apparent from the terms of Directive 2001/29/EC that it is contemplating the grant of an injunction upon the application of rights holders, yet the claimants are seeking an injunction to restrain activities in relation to all binary and all text materials in respect of which they own no rights and about which I have heard little or no evidence. Second, I do not accept that the defendant has actual knowledge of other persons using its service to infringe all such rights. Therefore I am not persuaded I have the jurisdiction to grant such an injunction in any event. Third, the rights of all other rights holders are wholly undefined and consequently the scope of the injunction would be very uncertain." *Newzbin2* (Twentieth Century Fox), [2011] EWHC 1981 ¶ 151 (citing *Newzbin*, [2010] EWHC 608 ¶ 135).

[24] "In the digital environment, in particular, the services of intermediaries may increasingly be used by third parties for infringing activities. In many cases such intermediaries are best placed to bring such infringing activities to an end." Directive 2001/29, 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 (L167) 10, 15 (EC).

[25] *Newzbin2* (Twentieth Century Fox), [2011] EWHC (Ch) 1981 ¶ 185.

[26] *See id.* ¶ 155 (citing Directive 2004/48 of the European Parliament and of the Council of 29 April 2004 on the Enforcement of Intellectual Property Rights, 2004 O.J. (L 195) 16, 23 (EC); and E-Commerce Directive, *supra* note 5, at Art. 18).

[27] *See generally Newzbin2* (Twentieth Century Fox), [2011] EWHC (Ch) 1981 ¶ 156. The court was basing its opinion on the decision in the case of *L'Oreal SA & Ors v. Bellure NV & Ors* [2010] EWCA Civ 535, a trademark case which had several questions referred to the Court of Justice (E.U.) for guidance. The landmark decision from the European Court of Justice in which the court determined that packaging will infringe a trade mark registration if it is designed to mimic the registered right to gain a commercial advantage, even if consumers do not believe that the infringing goods originate from the brand owner. *Id.* ¶ 138.

[28] This order was the first of its kind in the United Kingdom and has led to a quick series of requests by industry. At the current time, Sky has also blocked access to Newzbin, stating: "We have received a court order requiring us to block access to this illegal website, which we did on 13th December, 2011." *Our*

¶9 Based on the *Newzbin* cases, one could argue that in the United Kingdom an ISP can be served with an injunction to shut down a website if the ISP has actual knowledge of widespread infringing activity, as demonstrated by either: (1) a large number of individuals, albeit not clearly identified, illegally downloading or uploading materials, and/or (2) a large number of illegally obtained files being uploaded or downloaded on a single website. According to the *Newzbin2* court, such an order can be given even if it is unclear who or what owns the rights being infringed and even if some right holders are not present or represented in the court action.[29] The court has taken no issue with the blocking of these types of websites most likely because the illegal behavior associated with the website is so widespread. However, the court's insistence that a service provider must "contribute to the prevention of further infringements" left many wondering about the full scope of what an Internet service provider must do to "contribute" to the prevention of intellectual property rights infringement.

III. THE SABAM BALANCING SCALES

¶10 The declaration of a court that an Internet service provider must "contribute" to the prevention of intellectual property infringements led to widespread confusion among the online community and to a flurry of activity on the part of intellectual property right holders requesting that service providers undertake policing activities. The *SABAM* case presented, for the first time, an opportunity for the ECJ to weigh in on the requirement that service providers contribute to the protection of intellectual property rights.

¶11 The *SABAM* case arose from an expected dilemma for ISPs: is it an ISP's responsibility to discover and prevent users from accessing services that assist in copyright infringing activities? It is important to note that some commentators and industry researchers describe the scale of loss associated with online piracy as frankly staggering.[30] While those outside the music and movie industry refute some of the

---

Approach to Protecting Copyright, SKY NEWS, http://www.sky.com/helpcentre/broadband/protecting-copyright/ (last visited 8/11/12). Two of the other popular internet providers within the United Kingdom, Virgin Media and TalkTalk, have also been asked by the Motion Picture Association to block access to Newzbin. Both have indicated that they would do so in response to a court order. *See Sky, Virgin Media Asked to Block Piracy Site Newzbin2*, BBC ONLINE (Nov 9, 2011), http://www.bbc.co.uk/news/technology-15653434. In one of the most recent blocking orders, in April of 2012 the English High Court issued an order to Sky, Everything Everywhere, TalkTalk, O2, and Virgin Media requiring the ISPs to prevent their users from accessing the website known as Pirate Bay. *See The Pirate Bay must be blocked by UK ISPs, Court Rules*, BBC ONLINE (April 30 2012), http://www.bbc.co.uk/news/technology-17894176. Microsoft Windows has voluntarily followed suit in preventing links to the Pirate Bay website from appearing in Messenger. *See Microsoft Windows Messenger blocks The Pirate Bay link*, BBC ONLINE (March 27, 2012), http://www.bbc.co.uk/news/technology-17524815. It is very possible that Pirate Bay will be more widely blocked as the site appears to be the subject of a deepening investigation by the Swedish authorities. *See Swedish Investigation into The Pirate Bay 'Deepens'*, BBC ONLINE (March 15, 2012), http://www.bbc.co.uk/news/technology-17387858.

[29] *See Newzbin2* (Twentieth Century Fox), [2011] EWHC (Ch) 1981 ¶ 148.

[30] As the *Newzbin2* court highlights: "A study by Ipsos MediaCAT dated April 2010 analyzing the scale of film and television piracy in the UK in 2009 estimated the overall loss from film piracy at £477 million and the overall loss from television piracy at £58 million. A study by Tera Consultants dated March 2010 concluded that in 2008 the audio and audiovisual industries in the UK lost almost 670 million euros in revenues to physical and digital piracy, with the larger proportion of that lost revenue attributable to digital piracy." *Newzbin2* (Twentieth Century Fox), [2011] EWHC 1981 ¶ 20.

numbers concerning the scale of infringing activity,[31] one can appreciate the reactions of various industries impacted by the violation of intellectual property rights. Even if we assume a conservative number, it's no surprise that ISPs are in the cross hairs of the music, television, and film industries, which are being bled by online piracy and claim that their only hope of stemming the tide is to prevent the wide-scale distribution of pirated material online. Consequently, some argue, it is not merely enough to craft injunctions that shut down people and websites actively engaging in copyright infringement; it is also important to require intermediaries—such as ISPs—to take preventative measures. ISPs, meanwhile, fear this argument, insisting that it will burden them with the frankly unrealistic duty to monitor all online activity.

¶12 The *SABAM* case provides a perfect example of the dilemma that ISPs face and the balance that must be struck between the rights of all in the online world. In 2004, SABAM[32] discovered that subscribers to the Belgian ISP Scarlet Extended (Scarlet) were using the ISP's services to illegally download, through P2P networks, protected works from its catalogue, without authorization and without paying royalties.[33] SABAM thus requested that a Belgian Court issue an injunction against Scarlet forcing it to block any such downloading or uploading of illegal files via P2P networks without authorization.[34] In June of 2007, the Brussels Court of First Instance granted the injunction and ordered Scarlet to ensure that no copyrighted works were downloaded. Failing to do so would mean paying a daily fine.[35] Scarlet appealed the ruling, arguing that imposing an obligation to monitor the activities of its users is incompatible with the E-Commerce directive and with fundamental rights[36] enshrined within E.U. law. The Brussels Appeal Court proceeded to ask the European Court of Justice whether E.U. law[37] precludes an injunction asking an ISP to filter for copyrighted content with a view to blocking the transfer of those files, including the use of filters as a preventative measure.[38] In responding to the question, the ECJ goes to great lengths to consider the potential conflict between several E.U. Directives concerning information, intermediaries, copyright rights holders,[39] and the European Convention on the Protection of Human Rights and

[31] *See, e.g.*, IAN HARGREAVES, DIGITAL OPPORTUNITY: A REVIEW OF INTELLECTUAL PROPERTY AND GROWTH (2011), *cited in SABAM*, C-70/10 ¶ 21.

[32] One should note I have had to rely upon the ECJ case and *Newzbin2* for the basic summary. *See SABAM*, C-70/10 ¶¶ 15-28; *Newzbin2* (Twentieth Century Fox), [2011] EWHC 1981 ¶¶ 165-77.

[33] *See SABAM*, C-70/10 ¶ 17.

[34] *See id.* ¶ 18.

[35] *See id.* ¶ 23.

[36] *See id.* ¶ 27.

[37] *See id.* ¶ 28. The E.U. law being: (1) the 2000 E-Commerce Directive, *supra* note 5; (2) the 2001 Directive for Copyright harmonisation, (3) the 2004 Directive on the Enforcement of Intellectual Property Rights, (4) the 1995 Directive on Data Protection and (5) the 2002 Directive on Data Protection in the field of Electronic Communications.

[38] Reference (OJ) OJ C 113 of 01.05.2010, p.20, *available at* http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=EN&Submit=rechercher&numaff=C-70/10.

[39] *See* Directive 2001/29 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, 2001 (O.J. L 167) 10; Directive 2004/48 of the European Parliament and of the Council of 29 April 2004 on the Enforcement of Intellectual Property Rights, 2004 (O.J. L 157) 16; Directive 95/46/EC of the European Parliament and 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, 1995 (O.J. L 281) 31; Directive 2000/31 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 (Directive on Electronic Commerce),

Fundamental Freedoms, specifically the protection of copyright and the protection of the fundamental rights of individuals.[40] In making its determination, the *SABAM* court recognized two fundamental issues in relation to service providers: (1) the court affirmed existing E.U. case law and academic commentary placing service providers in a position to "cooperate" with intellectual property right holders in protecting copyright in the online world, and (2) it began to establish the balance that must be maintained between a service provider's rights and intellectual property holder's rights.

¶13 In determining the parameters of this balance, the *SABAM* court declared: "[T]he protection of the fundamental right to property, which includes the rights linked to intellectual property, must be balanced against the protection of other fundamental rights."[41] Fortunately, the court recognized the need to be more proscriptive in such an evolving area of law and went on to focus on three fundamental rights within the E.U. that must be considered in creating the balance: (1) the right of business to conduct its business,[42] (2) the right of an individual to protect personal data,[43] and (3) the right of an individual to receive and impart information.[44] Consequently, the interests of intellectual property rights holders must be balanced against the right of service providers to conduct business, the right of the individual to protect personal data, and the right of the individual to receive and impart information. And because the weight of each set of rights shifts on a case-by-case analysis, one can imagine a scale shifting the balance based on the specific facts of the circumstances presented.

¶14 Post-*SABAM*, the first pressing issue is what percentage of unlawful activity is enough to shift the *SABAM* balance so significantly that the intellectual property right holder's interest is given prominence? Unsurprisingly, most commentators argue that all of the websites previously discussed are hosting widespread copyright infringing activities by their users. Consequently, the blocking of Newzbin, Newzbin2, and Pirate Bay sites were not controversial. But what if the website had contained 40% non-infringing use? What if the number is closer to 60%? Where is the line? The answer, of course, has to be determined on a case-by-case analysis of the particulars of the websites and the activities of the websites users. Clearly, 90% infringing activity by users is strong support for a blocking order. However, this line is not as easy to define, as part of the first consideration must be in relation to the definition of what constitutes infringing activity. What happens when a website has 90% of its users uploading legal material and only a few outliers uploading a large amount of infringing material? Is this to be treated

---

2000 (O.J. L 178) 1; Directive 2002/58 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 (Directive on Privacy and Electronic Communications), 2002 (O.J. L 201) 37.

[40] *See* Convention on the Protection of Human Rights and Fundamental Freedoms, art. 8, 10, Nov. 4, 1950 (as amended June 1, 2010).

[41] *SABAM*, C-70/10 ¶ 44.

[42] *See id.* ¶ 46 (citing Charter of Fundamental Rights of the European Union, art. 16, 200 O.J. (C 364) 1, 12).

[43] *See* Charter of Fundamental Rights of the European Union, art. 8 200 O.J. (C 364) 1, 10 ("Everyone has the right to the protection of personal data concerning him or her"); *id.* at 11 ("Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.").

[44] E-Commerce Directive, *supra* note 5 at 6. (The recitals to the E-Commerce Directive note, "the removal or disabling of access has to be undertaken in the observance of the principle of freedom of expression.").

the same as a website with many users infringing copyright? The answer is no. A website with only a few members uploading and/or downloading a large amount of infringing material should be attacked via action against the individuals. Websites should only be shut down when a large number of individual users are perpetrating a large amount of illegal activity. Without this restriction, the original laws designed to prevent individual users from widespread infringement are superfluous. Moreover, the overzealous use of this new method of attack may result in curbing legal and lawful uses in relation to the sharing of information online.

¶15 Concerning the burden that an Internet service provider[45] must undertake to cooperate in the protections, courts have already established several important factors to be considered in the shifting balance. In a similar manner to the telephone company, Internet service providers should not be expected to undertake general monitoring of its customers' behavior.[46] Even in a situation where monitoring activities become less costly,[47] an ISP should not be expected to be anything more than a provider of a communications service that is in a position to help, but should not be burdened by, the assertion of intellectual property rights. Thus far, courts have considered the following factors relevant to determining the burden ISPs should bear: cost of implementation,[48] cost associated with upkeep, cost associated with monitoring,[49] level of data inspection required,[50] complexity of the system to be installed,[51] duration of the request,[52] and the technical feasibility of such a request.[53] Internet service providers cannot be asked to implement a system that monitors all information,[54] for an unlimited time,[55] at the

[45] Other courts have considered a different balance. For example, in the U.S., Judge Posner used a cost-and-benefit analysis when considering the service provider's role in the protection of intellectual property rights. In the case of *In re Aimster Copyright Litigation*, Judge Posner set forth a "disproportionately costly" test, stating: "[I]f the infringing uses are substantial then to avoid liability as a contributory infringer the provider of the service must show that it would have been disproportionately costly for him to eliminate or at least reduce substantially the infringing uses." *In re Aimster Copyright Litigation*, 334 F.3d 643, 653 (7th Cir. 2003).

[46] The Court in *L'Oreal SA & Ors v. Bellure NV & Ors* specified that national measures which require an intermediary provider, such as an ISP, to actively monitor all the data of each of its customers in order to prevent any future infringement of intellectual-property rights violates this general monitoring provision. *See L'Oreal SA & Ors*, [2010] EWCA (Civ) 535 ¶ 139 (citing Directive 2004/48, Article 3 (2)).

[47] The *SABAM* court specifies that even in the face of less costly measures, the balance would still not tip in favor of requiring ISPs to monitor customers' online activity. As the court highlights: the injunction would "require the ISP to carry out general monitoring, something which is prohibited by Article 15(1) of Directive 2000/31." *SABAM*, C-70/10 ¶ 40.

[48] *See id.* ¶ 48.

[49] The Court highlights the installation of the filtering system would require that ISP to "install a complicated, costly, permanent computer system at its own expense." *Id.* ¶ 48.

[49] *See id.* at ¶ 47.

[50] *See Newzbin2* (Twentieth Century Fox), [2011] EWHC (Ch) 1981 ¶ 162.

[51] The Court emphasizes that the implementation of such a system would also be contrary to the conditions laid down in Article 3(1) of Directive 2004/48 which requires that measures to ensure the respect of intellectual-property rights should not be unnecessarily complicated or costly. *See SABAM*, C-70/10 ¶ 36 (citing *L'Oreal SA & Ors*, [2010] EWCA (Civ) 535 ¶ 139).

[52] The Court seems unwilling to expect an intermediary to undertake such an expense when the "monitoring has no limitation in time, is directed at all future infringements and is intended to protect not only existing works, but also future works that have not yet been created at the time when the system is introduced." *See SABAM*, C-70/10 ¶ 47.

[53] *See id.*

[54] *See id.*

exclusive cost of the ISP.[56] Such a general order would place an undue burden on service providers that should be considered a significant barrier to the operations of the service providers' business.[57] However, a specific, targeted, and precise injunction requiring the use of an existing technology to monitor behavior is a reasonable burden.[58]

¶16 One is left to wonder, however, if the court-prescribed balance between intellectual rights holders, businesses, and customers can be adequately accomplished when the filtering or blocking mechanism employed "over captures" lawful content[59] and, in doing so, over burdens the rights of individuals. The ECJ highlights that blocking lawful activity might undermine the freedom of information protections enshrined in the E.U. Charter of Fundamental Rights (Art 11)[60] by preventing individuals from accessing their lawfully created and owned information, communications of personal videos.[61] And because over capturing impacts individuals in this manner, individuals and their rights are an important part of the balance that courts must begin to consider. This issue may be precisely what the *SABAM* court was intending to highlight: what happens when the system over captures customers' communications such that lawful activity and information is now blocked.[62] This issue is highlighted by the attorneys for Kyle Goodwin in *United States v. Kim Dotcom and Megaupload Limited*[63] (*Megaupload*):

> It is one thing to take legal action against an alleged copyright infringer. It is quite another to do so at the expense of entirely innocent third parties, with no attempt to prevent or even mitigate the collateral damage.[64]

As noted by Goodwin's attorney, the problem of over capturing is exacerbated as the law does not provide for protections of individuals' information or communications.

---

[55] *See id.*

[56] *See id.* ¶ 48. The Court emphasizes that the implementation of such as system would also be contrary to the conditions laid down in Article 3(1) of Directive 2004/48, which requires that measures to ensure the respect of intellectual-property rights should not be unnecessarily complicated or costly. *Id.*

[57] *See id.* ¶ 47-48.

[58] *Newzbin2* (Twentieth Century Fox), [2011] EWHC 1981 ¶ 177.

[59] *See SABAM*, C-70/10 ¶ 52.

[60] *See* Charter of Fundamental Rights of the European Union, 2000 O.J. (C 364) 11, http://www.europarl.europa.eu/charter/pdf/text_en.pdf.

[61] The ECJ emphasizes that ISP customers are guaranteed the freedom to receive and impart information. Filtering mechanisms, such as those described in this case, might not adequately distinguish between unlawful content and lawful content. The practical result of such an implementation is the blocking of lawful communications. *See SABAM*, C-70/10 ¶ 52.

[62] *See SABAM*, C-70/10 ¶ 52.

[63] *See* Indictment, United States v. Dotcom, No. 1:12-3 (E.D. Va. Jan. 5, 2012), *available at* http://www.citmedialaw.org/sites/citmedialaw.org/files/2012-01-05-Indictment.pdf. The term Megaupload is being used in this article as it is the most recognizable name used in the media. However, the "conspiracy" involved numerous other websites and, of course, several named individuals. The Los Angeles Times has produced numerous stories on the topic and has a full version of the court indictment. *See, e.g.*, Nathan Olivarez-Giles, *Justice Department Indictment of MegaUpload*, LOS ANGELES TIMES (Jan. 19, 2012), http://documents.latimes.com/justice-department-ndictment-file-sharing-site-megaupload/.

[64] Brief of Interested Party Kyle Goodwin at 1, United States v. Dotcom, No. 1:12-3 (E.D. Va. Mar. 30, 2012), *available at* https://www.eff.org/sites/default/files/filenode/MegauploadMotion-1.pdf. *See also*, Greg Sandoval, *U.S. Tries to Silence MegaUpload Lawyers on Issue of User Data*, CNET NEWS (April 13, 2012), http://news.cnet.com/8301-1023_3-57413506-93/u.s-tries-to-silence-megaupload-lawyers-on-issue-of-user-data/; David Kravets, *Judge Won't Purge Megaupload User Data, At Least Not Yet*, WIRED (April 13, 2012), http://www.wired.com/threatlevel/2012/04/megaupload-data-flap/.

Although the U.S. does provide such protections when an individual's information/communication is removed from a website,[65] no law in the E.U. or U.S. provides protections in the event that an entire website is blocked.[66] Consequently, in the absence of legal proscriptions, the courts must craft ways to protect the lawful information and/or communications captured within a shut-down/block order. At a minimum one would expect that the shutdown order would require: (1) that a filtering or similar system be set up to remove from the block and return to the rightful owner any information/contents or communications that are clearly not the subject of an intellectual property rights holder claim against the website/user, (2) a provision for the individual that stored or transmitted the information to demonstrate that the contents are of a lawful use/activity, and (3) the safekeeping of the information until any issues are resolved. Balance is struck in these instances only when information is protected and when retrieval of lawful information is possible.

¶17 If European law better handled the over-capturing issue, would the *SABAM* balance place less of an emphasis upon the rights of the individuals and their lawfully stored information? If these protections existed, either through E.U. action or individual court action, one could argue that the over-capturing issue would be less significant within the *SABAM* balance. In fact, it is easy to imagine the elimination of the concerns in relation to individuals and the protection of their information that currently takes a high level of prominence within the *SABAM* balance considerations.

¶18 Moreover, returning to the issue of cost in relation to the captured information/communications, it is reasonable that any court order blocking a website would require the website's host to bear the cost of setting up a system that filters out users' lawful information and the cost of storing legal information while the dispute is resolved. But again, as this is an unresolved issue, the law fails to fully flesh out the cost burden of storing and protecting information. The *Megaupload* court in the U.S. is currently considering this issue.[67] Meanwhile, as legislation seeks to catch up with the

[65] The DMCA provides specific protections in relation to individuals' disabled or removed information, including rights in relation to challenging such removal, under the concept known as counter-notice. *See generally* Edward Lee, *Decoding the DMCA Safe Harbors*, 32 COLUM. J. L. & ARTS 233 (2009) (discussing the use of safe harbor protections); Lydia Pallas Loren, *Deterring Abuse of the Copyright Takedown Regime by Taking Misrepresentation Claims Seriously*, 46 WAKE FOREST L. REV. 745 (2011) (determining that copyright owners obtain prompt removal of infringing material from the Internet without judicial assessment of the assertion of infringement); Ira S. Nathenson, *Looking for Fair Use in the DMCA's Safety Dance*, 3 AKRON INTELL. PROP. J. 121 (2009); Miquel Peguera, *The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems*, 32 COLUM. J.L. & ARTS 481 (2009) (comparing U.S. to European law).

[66] Interestingly, India has recently clarified a prior order which seemingly required ISPs to block the well-known website "Pirate Bay." In June, the Madras High Court of India clarified the order to block the site, stating: "[T]he interim injunction is granted only in respect of a particular URL where the infringing movie is kept and not in respect of the entire website." *India Unblocks the Pirate Bay and Other Sharing Sites*, BBC (June 22, 2012), http://www.bbc.com/news/technology-18551471.

[67] *See* Kravets, *Megaupload User Data*, *supra* note 65; David Kravets, *Retired Judge Joins Fight Against DOJ's 'Outrageous' Seizures in Megaupload Case*, WIRED (June 13, 2012), http://www.wired.com/threatlevel/2012/06/retired-judge-megaupload/; *Megaupload User Asks Court to Return His Video Files*, ELECTRONIC FRONTIER FOUNDATION (Mar. 30, 2012), https://www.eff.org/press/releases/megaupload-user-asks-court-return-his-video-files; Jacob L. Rogers, *U.S. v. Kim Dotcom: Government Says Megaupload Users Must Pay to Retrieve Their Data*, JOLT DIGEST, (June 18, 2012, 6:48 AM), http://jolt.law.harvard.edu/digest/copyright/u-s-v-kim-dotcom; Greg Sandoval, *EFF to Federal Court: Return MegaUpload Data Now*, CNET (May 25, 2012, 9:32 AM), http://news.cnet.com/8301-1023_3-57441702-93/eff-to-federal-court-return-megaupload-data-now/;

evolving case law, courts should consider the balance of costs associated with the protection of legal data and should pass on costs associated with the storage and maintenance to the offending website hosts. The courts must seek to achieve the balance.

¶19 In summation, to achieve the *SABAM* balance requires the availability of technology that is not too costly to monitor, install, or maintain. There would also have to be mechanisms put in place to protect information stored on a website when it is being blocked. Additionally, achieving the *SABAM* balance would require a system to filter lawful material and return it to its owner in a timely manner and to ensure the law abiding users of a website to resolve issues in a timely manner. Finally, legal information would need to be maintained while all of these issues were resolved. Few of these mechanisms or protections currently exist. Consequently, the *SABAM* balance is much more difficult to achieve then it may appear at first blush.

IV. ONGOING PROBLEMS

¶20 The *SABAM* decision has raised more questions than it has provided answers. However, the case did achieve clarity in relation to one pressing issue: namely, that service providers must cooperate in protecting intellectual property rights but may not be overburdened by this requirement. Unfortunately, many of the unresolved issues will cause ongoing problems. In fact, some of the SABAM court's resolutions may have created more problems in this fast moving area of law.

A. Adherence to the Prescribed Balance is Not the Answer

¶21 The court in *SABAM* used a traditional legal prescription to resolve the issues it faced, namely the need to balance fundamental rights between three parties: the intellectual property right holders, individuals and business (ISPs).[68] But such a balance seems to suggest in most instances that the various positions must be in conflict with one another. This is an odd thought concerning fundamental rights. If we think of intellectual property rights and other fundamental rights as balanced on a scale, a loss in the fundamental rights side is *ipso facto* a gain for the other side. However, in light of the various cases discussed above, should a balance be required at all? In a large majority of the situations, there is no conflict between rights and thus a balance is not the appropriate standard to be used within the courts consideration. For example, in the case that an individual illegally downloads a copy of the final episode of *Desperate Housewives*, the individual knows the action is copyright infringement but fails to appreciate this action as theft of another's property.[69] The individual has no right in the intellectual property and is owed no considerations of balance in relation to the illegal online activity. The

Sandoval, *U.S. Tries to Silence MegaUpload Lawyers*, *supra* note 65.

[68] *See SABAM*, C-70/10.

[69] *See* Oliver Goodenough & Greg Decker, *Why Do Good People Steal Intellectual Property?*, 14-15 *in* THE GRUTER INSTITUTE WORKING PAPERS ON LAW, ECONOMICS, AND EVOLUTIONARY BIOLOGY (Vol. 4 2007), *available at* http://www.bepress.com/giwp/default/vol4/iss1/art3 (arguing that the different attitudes towards intellectual and tangible property are due to an insufficient affective component to the understanding of intellectual property rights with most people); Alexander Peukert, *Why Do "Good People" Disregard Copyright on the Internet?*, *in* CRIMINAL ENFORCEMENT OF INTELLECTUAL PROPERTY: A HANDBOOK OF CONTEMPORARY RESEARCH, (Christophe Geiger ed., forthcoming Dec. 2012) (manuscript at 14) ("digital sharing is an everyday practice by millions of people, and in that sense *normal*").

individual justifies his actions by claiming that copyright law has failed to keep up with the online world and needs reform, or that everyone is doing it,[70] or he rationalizes his actions as appropriate because it is the fault of the various industries for not understanding the demands of their customers.[71] There is no need to balance; the individual has no right to download or upload information or communications that are not identified by the law as belonging to him regardless of his justifications or rationalizations of his illegal activity. While naysayers may insist that copyright law must be reformed (they are right)[72] and that the entertainment industry must respond to users' appetite for quick and reasonably priced access to music and movies (also right),[73] current law prohibits downloading or uploading information that is protected by another's intellectual property rights. The individual should seek to change the law in relation to intellectual property, but violations of the law should not be entertained, nor are the activities deserving of considerations of the need to balance rights amongst parties.

¶22 In the case that an Internet service provider or other entity denies an individual or business access to its lawfully created material, such as in the Megaupload case, the online entity is in violation of the law. The information and communication belongs to the individual. Denying the individual or business access to its personally created Word document or video is an infringement of the individual's fundamental property right.[74] Again, there is no need to balance the rights; the rights are clear and do not conflict.

¶23 In terms of the potential to consider a service provider's right to conduct business as an area to be balanced against the intellectual property holder rights, again this is ultimately not resolved through the use of creating a balance. Like any other business in the E.U., a service provider has a right to conduct business, but only when doing so does not enable or promote unlawful activity. There are no balance considerations necessary. Instead, the question is how much burden is reasonable for an Internet service provider to undertake when faced with the *illegal* activity of its customers.

B. Overburdening Internet Service Providers is Not the Answer

¶24 ISPs have a fundamental right to operate their business without an undue burden. But what constitutes an undue burden? As the courts continue to struggle with this question on a case-by-case basis, some wonder if the burden of protecting intellectual property rights placed on service providers should include considerations of the high volume of activity being requested to protect intellectual property rights.

---

[70] *See* John Palfrey, Urs Gasser, Miriam Simun & Rosalie Fay Barnes, *Youth, Creativity, and Copyright in the Digital Age*, INT'L J. OF LEARNING AND MEDIA 79, 87 (2009).

[71] *Id.* at 89. Another theory is one of moral disengagement, where individual "users reconstruct their conduct as having a moral purpose in order to make it socially acceptable." Peukert, *supra* note 70 (manuscript at 16).

[72] *See, e.g.*, Stacy Baird, *Contentious Issues: Copyright Reforms in the Age of Digital Technologies* 1 (Working Paper), *available at* http://ssrn.com/abstract=1520161 ("Copyright holders and users of copyrighted works alike believe changes to copyright law are imperative to maintain the social benefits of copyright law.").

[73] *See, e.g*, Rob Reid, *What To Do When Attacked by Pirates*, WALL ST. J. (June 1, 2012, 7:02 PM), http://online.wsj.com/article/SB10001424052702303552104577438212250619458.html?mod=wsj_share_tweet.

[74] *See supra* notes 61-63 and corresponding text.

¶25 British Telecommunication (BT) estimates that the court order to block the Newzbin website cost £5,000 (U.S. $7,865) to implement.[75] While this may seem a small cost in light of BT's annual earnings,[76] it is not a cost BT should bear. Moreover, this is the cost for a single implementation of a website blocking order. Should the courts consider the burden in a more "big picture" holistic manner? In other words, should the courts consider not only the cost of a single event but rather consider the totality of all activities that a service provider must undertake to protect intellectual property rights? If BT has a fundamental right to not have its business unduly burdened, surely a holistic approach is necessary as it is only in this light that the true nature of the burden becomes apparent. The creation of a holistic burden approach demands that courts consider the entire burden of requiring ISPs to protect intellectual property rights. One such burden is intellectual property right holders' "take down" requests. Consider the statements made by Verizon Communications:

> While Verizon receives valid "notice and takedown" requests from copyright owners and responds promptly with the "take down" and counter-notification processes, we have unfortunately also experienced increasing misuses of the Designated Agent information located on the Copyright Office's website. The misuses fall into a variety of categories, including cases of (i) P2P and other file sharing activities where the material alleged to be infringed does not reside on a service provider's system or network, yet ISPs are often sent automated "takedown" notices by the thousands; (ii) allegations of trademark infringement, where the DMCA "notice and takedown" provision does not apply; (iii) material that is protected by the "fair use" defense of the Copyright Act; and (iv) abusive litigation tactics made in the alarming growth of "copyright troll" lawsuits.[77]

¶26 In other words, ISPs are being inundated with take down requests, some legitimate and some clearly nothing more than nefarious attempts to restrict the use of material or to catch ISPs without timely take down response procedures.[78] Some of these issues are distinguishable from the issue at hand, as the requests Verizon notes are not in response to a court order but a mere "good faith" request to remove copyrighted material. Yet it is still worth asking: in examining the proper degree of burden placed on a business, shouldn't a holistic consideration include the entirety of the burden placed on ISPs to protect online intellectual property rights?

---

[75] *See* Rich Trenholm, *Newzbin BT ban demanded for Sky, Virgin Media and TalkTalk*, CNET, (Nov 9, 2011, 5:19 PM), http://crave.cnet.co.uk/software/newzbin-bt-ban-demanded-for-sky-virgin-media-and-talktalk-50006004/.

[76] BT's earnings were estimated at over 1.8 billion in 2012. *See Annual Financials For BT Group*, PLC ADS, MARKET WATCH, http://www.marketwatch.com/investing/stock/bt/financials (last visited Dec. 1, 2012).

[77] Sarah B. Deutsch, *Re: Request for Public Comment on Designation of Agent to Receive Notification of Claimed Infringement*, UNITED STATES COPYRIGHT OFFICE 2 (Nov. 28, 2011), *available at* http://www.copyright.gov/docs/onlinesp/comments/2011/initial/verizon.pdf. *See also* Ke Steven Wan, *Managing Peer-to-Peer Traffic with Digital Fingerprinting and Digital Watermarking*, 41 SW. L. REV. 331 (2012) (arguing that the graduated response system will aggravate the misuse of the notice-and-takedown procedure and strengthen the content industry's control over content).

[78] *See* Nathenson, *supra* note 66, at 168.

¶27 Taken together, court orders and "good faith" take-down requests create an unfair burden for ISPs as the cost alone is prohibitive.[79] These requirements grate against the original idea of copyright holders bearing the burden of identification and enforcement costs in protecting intellectual property rights.[80] No amount of court ordered "cooperation" should shift the burden or protect intellectual property rights to such a large extent. This fundamental shift redistributes the burden of protecting intellectual property rights to the ISP, which, in the long run, may overtake a large portion of the time commitments of the ISP, add undue cost, and may effectively shut down some ISPs and/or websites.

¶28 Moreover, one can appreciate that the rise in take down requests is a likely result of an inefficient and unsuccessful law that requires constant court intervention to stop widespread copyright infringement. Without a level of clarity and legal reform in the area of online intellectual property rights it is easy to imagine an increase in take-down, shut-down, and removal requests. The system is sagging at the seams and one of the parties bearing a large part of the burden of policing and responding to intellectual property rights holders' concerns is service providers. The balance has fundamentally shifted, more than the *SABAM* court could have ever imagined or considered in light of the case before it. The sheer weight of the activity being required of service providers to police the Internet for copyright infringement should be considered an undue burden.

C. Ongoing and Continuous Court Involvement is Not a Long-Term Solution

¶29 Currently, European Union Member States have differing laws concerning copyrighted works, especially relating to statutory exceptions to copyright. For example, some Member States classify certain works as falling within the public domain,[81] while others allow works to be posted online free of charge[82] with little concern to copyright protections. The fact that E.U. law remains fragmented on copyright issues is a concern of service providers, as highlighted by the *SABAM* court:

> Indeed, it is not contested that the reply to the question whether a transmission is lawful also depends on the application of statutory exceptions to copyright which vary from one Member State to another.[83]

¶30 The perplexities of legal protections are just as diverse among all jurisdictions.[84] For example, Canada is in the midst of reforming its copyright laws;[85] the European

[79] *See* Peter K. Yu, *The Graduated Response*, 62 FLA. L. REV. 1373, 1392 (2010) ("If ISPs were to fully investigate the potential infringing activities, the costs of such investigation could be prohibitive.").

[80] *See* Anna Katz, *Copyright In Cyberspace: Why Owners Should Bear The Burden Of Identifying Infringing Materials Under The Digital Millennium Copyright Act*, B.U. J. SCI. & TECH. L. 18.2 (2012) (discussing the DMCA and the burdens assumed within the creation of protections).

[81] *See SABAM*, C-70/10 ¶ 52.

[82] *See id*.

[83] *Id*.

[84] *See e.g.*, Peguera, *supra* note 66, at 481.

[85] For a broad discussion of the new Canadian Bill C-11 (Copyright Reform), see Michael Geist, *Conclusion Of Copyright Debate Leaves Many Unanswered Questions*, THESTAR.COM (May 26, 2012), http://www.thestar.com/business/article/1196810--conclusion-of-copyright-debate-leaves-many-unanswered-questions.

Commission plans to examine procedures used to take down copyright-infringing and other illegal content from websites;[86] Germany has criminalized copyright infringement;[87] Norwegian copyright protections are limited by privacy rights;[88] and the United States stands ready to go to great lengths to protect intellectual property rights,[89] even through the application of criminal law. Given this complexity, it is not surprising that service providers insist upon a court order, as the potential of liability arising from misreading or misunderstanding these complex areas of law will subject the ISPs to liability from all parties concerned.

¶31 But mere court involvement may not be enough, as noted by the 108 law professors in their letter to Congress entitled "Letter in Opposition to 'Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011 (PROTECT IP Act).'"[90] The language of the PROTECT IP Act requires Internet service providers to refuse to recognize Internet domain names that a court considers "dedicated to infringing activities."[91] While a noble and appropriate goal, the Act allowed courts, with nothing more than a temporary restraining order and without the requirement of a basic hearing, to order any Internet service provider to stop recognizing sites. It is easy to understand why ISPs would find this worrisome. Shutting down a website should require court involvement and not just a mere application to the court.

¶32 The Protect IP Act, in an attempt to react quickly to a widespread infringing activity occurring on various websites, has compromised the due process rights of service providers, online users, and the online community as a whole. Such willingness to circumvent due process is an example of the extreme measures being proposed to react to a fast-evolving online world. If such legislation is to be promulgated as a response to the speed required to effectively shut down websites that promote copyright infringement, the courts must be involved to protect due process considerations. However, court involvement—even under the Protect IP Act—is expensive and takes time. Copyright

---

[86] In making this announcement, the European Commission noted that this public consultation is part of a much larger new e-commerce action plan. The new plan will examine everything from copyright to the basics of e-commerce and cyber security in an effort to "doubl[e] the share of e-commerce in retail sales (currently 3.4 percent) and that of the internet sector in European GDP (currently less than three percent) by 2015." *Commission Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A Coherent Framework for Building Trust in the Digital Single Market for E-commerce and Online Services*, COM (2011) 942 final (Jan. 11, 2012).

[87] Although, in the case of an individual, non-commercial or small scale infringement of the law is not enforced. *See* Peukert, *supra* note 70 (Manuscript at 4).

[88] This is contentious in many EU jurisdictions. *See generally* Baird, *Contentious Issue*, *supra* note 73. In fact, Norwegian Minister of Education, Bård Vegar Solhjell, wrote on his personal blog that non-commercial file-sharing should be legalized in Norway and a blanket license scheme should be set up so creators are paid; writing that there is "no future in fighting" file-sharing services. Bård Vegar Solhjell, *Lovleg fildeling med Tono-avgift, (file sharing with a fee)*, BLOG OF BÅRD VEGAR SOLHJELL (February 18, 2009), http://www.bardvegar.no/2009/02/lovleg-fildelingmed-tono-avgift, *cited and translated in* Baird, *supra* note 73, at 53.

[89] *See* Megaupload discussion, *supra* note 64 and corresponding text.

[90] Professors' Letter in Opposition to "Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011" to members of the United States Congress (July 5, 2011), *available at* http://blogs.law.stanford.edu/newsfeed/files/2011/07/PROTECT-IP-letter-final.pdf. *See* Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011 (PROTECT IP Act of 2011), S. 968, 112 Cong. (2011).

[91] *See* Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011 (PROTECT IP Act of 2011), S. 968, 112 Cong. §3(b)(1), (2011).

holders have long complained that the "cost of seeking a blocking injunction under existing legislation is . . . prohibitive for all but the largest copyright owners."[92] And there are few alternatives, as service providers would subject themselves to liability for not insisting upon a court order. Clearly, court involvement is a necessary evil of the current system. But one must wonder if the system will ever actually achieve the goal of preventing—or even reducing—online infringing activity, given the cost and time involved with going to court.

D. Criminalizing the Service Provider is Not the Answer

¶33 The case of *United States v. Kim Dotcom and Megaupload Limited*[93] provides the clearest guidance to the U.S. position on websites that host ongoing and widespread infringing activities.[94] Megaupload is one of a series of websites owned by the now infamous Kim "Dotcom" Schmitz that allows customers to upload content into a cyber-locker. Various other Mega websites allowed everything from video streaming to online music storage.[95] Needless to say, the various websites were allegedly used to upload and stream material that was not appropriately licensed. Although Megaupload is a Hong Kong-based company, its web hosting company, Carpathia, is located in Virginia.[96] The physical location of a web hosting service in Virginia arguably gives the Virginia court jurisdiction over Megaupload activities related to storage and use of its server. Responding to what was viewed as widespread copyright infringing activities in the United States, the Justice Department seized several of the websites.[97] The five-count indictment, which alleges criminal copyright infringement as well as conspiracy to commit money laundering and racketeering,[98] described a site "designed specifically to

[92] *Site Blocking to Reduce Online Copyright Infringement: A Review of Sections 17 and 18 of the Digital Economy Act*, OFCOM, 6 (May 27, 2010), http://stakeholders.ofcom.org.uk/binaries/internet/site-blocking.pdf. In fact, substantial research exists in this area, focusing on the criminal statutes and corresponding effect of implementation and enforcement in Germany. *See*, Peukert, *supra* note 70.

[93] *See* Indictment, *supra* note 64.

[94] Megaupload is the most notorious, but not the only, website that has been seized in this manner. *See, e.g.*, Press Release, U.S. Immigration and Customs Enforcement (ICE), New York Investigators Seize 10 Websites That Illegally Streamed Copyrighted Sporting And Pay-Per-View Events (Feb 2, 2011), *available at* http://www.ice.gov/news/releases/1102/110202newyork.htm.

[95] The Federal Bureau of Investigation seized the Web site Megaupload and 18 domain names that formed Megaupload's network of file-sharing sites. *See* Ben Sisario, *7 Charged as F.B.I. Closes a Top File-Sharing Site*, N.Y. TIMES (Jan. 19, 2012), http://www.nytimes.com/2012/01/20/technology/indictment-charges-megaupload-site-with-piracy.html?_r=0.

[96] *See* Sandoval, *supra* note 65.

[97] *See FBI Anti-Piracy Warning*, http://megaupload.com/ (last visited Dec. 2, 2012). This is the most drastic of measures. In fact, in the United States, the DMCA is currently being used to block websites. *See* Weller, *supra* note 16.

[98] The indictment lists five criminal counts, all related to the underlying allegation of criminal copyright infringement. In addition to criminal copyright infringement (17 U.S.C. § 506 and 18 U.S.C. § 2319), the indictment alleges conspiracy to commit racketeering (18 U.S.C. § 1962) by being engaged in an enterprise to commit criminal copyright infringement, conspiracy to commit money laundering (18 U.S.C. § 1956) by transferring money that constituted the proceeds of criminal copyright infringement, and aiding and abetting criminal copyright infringement (18 U.S.C. § 2). The indictment alleges that Megaupload did not designate a copyright agent, as is required under the "safe harbor" of the Digital Millennium Copyright Act (17 U.S.C. § 512), and that Megaupload would deliberately avoid taking down an allegedly infringing file based on an infringement notice, opting instead to only delete the link to the file on which the complaint was based.

reward users who uploaded pirated content for sharing, and turned a blind eye to requests from copyright holders to remove copyright-protected files."[99] The result was a far-reaching indictment that effectively shut down Megaupload.com. The Megaupload case is just beginning to move through the courts, but four things should be noted: (1) criminal law was applied, (2) the law has yet to fully flesh out the use of criminal law in this manner, (3) this type of "international" criminal action is incredibly controversial,[100] and (4) the Department of Justice and the court have both intimated that the services hosting Megaupload sites may be the next entity pursued.[101]

¶34 Megaupload calls attention to several concerns relating to the use of criminal law to protect online intellectual property rights. The negative fury over the Anti-Counterfeiting Trade Agreement (ACTA)[102] highlights issues raised in relation to criminalization of activities of both ordinary users and third-party service providers. Although complaints and concerns about the Agreement are legion,[103] for the purpose of this paper I will focus on service providers. The current draft of ACTA eliminates provisions concerning the criminalization of both ordinary users and service providers.[104] The elimination of these provisions once considered essential to the Act is a key issue, as the removal of criminal law as a deterrent to infringing activity demonstrates strong and widespread disagreement amongst the drafters of the Act. Drafters clearly can find no consensus when determining the use of criminal sanctions against both individual users and service providers. Allowing either of these parties to be characterized as criminals or accomplices to criminal activity, without evidence of knowledge or willful participation in infringing activities, does not accomplish the end goal of reducing copyright infringing activity. Rather, it criminalizes an entire generation of Internet users, places too high of a burden on service providers, and ultimately impacts the manner in which Internet service providers operate. While this paper is not intended to focus on the need to protect individuals, criminalization of individual users has an impact on service providers. One could argue that criminalizing individual users will impact service providers because a service provider's failure to cooperate in the rooting out of online criminals may subject

[99] Nick Perry, *Popular File-Sharing Website Megaupload Shut Down*, USA TODAY (Jan. 20, 2012), http://www.usatoday.com/tech/news/story/2012-01-19/megaupload-feds-shutdown/52678528/1/.

[100] *See e.g.*, Mark Bartholomew, *Cops, Robbers, and Search Engines: The Questionable Role of Criminal Law in Contributory Infringement Doctrine*, 4 BYU L. REV. 783 (2009) (arguing against the use of criminal contributory infringement actions).

[101] *See* Greg Sandoval, *Judge Wants Megaupload User Data Preserved For Now*, CNET ONLINE, (April 13, 2012), http://news.cnet.com/8301-1023_3-57413693-93/judge-wants-megaupload-user-data-preserved-for-now/.

[102] *See* BBC News, Technology Section, *European Trade Committee Votes to Reject Piracy Treaty* (June 21, 2012), http://www.bbc.com/news/technology-18533268.

[103] *See e.g.*, David Kravets, *Anti-Counterfeiting Trade Agreement: Fact or Fiction?*, WIRED ONLINE, (Sept. 15, 2008), http://blog.wired.com/27bstroke6/2008/09/international-i.html; Connor Sheets, *ACTA vs. SOPA: Five Reasons ACTA is Scarier Threat to Internet Freedom*, THE INTERNATIONAL BUSINESS TIMES, (Jan. 24, 2011), http://www.ibtimes.com/acta-vs-sopa-five-reasons-acta-scarier-threat-internet-freedom-400004; *but cf.* ICC News Release, *Global Business Leaders Remind EU Leaders of Importance of ACTA to Economic Growth and Job Creation* (June 4, 2012), *available at* http://www.iccwbo.org/bascap/index.html?id=48503.

[104] *See* Erik Kain, *Final Draft of ACTA Watered Down, TPP Still Dangerous On IP Rules*, FORBES ONLINE (Jan. 28, 2012), http://www.forbes.com/sites/erikkain/2012/01/28/final-draft-of-acta-watered-down-tpp-still-dangerous-on-ip-rules/.

the service provider to liability. Thus, one could argue that neither individuals nor service providers should be criminalized.

¶35 Unfortunately, the *SABAM* courts failed to discuss the necessary balance between copyright protections predating and existing within the digital age. The absence of a realistic balance leaves service providers unprotected as they seek to navigate widely differing laws. In his 2007 TED Talk,[105] noted Professor Lawrence Lessig claims that the digital age has allowed the younger generations to re-engage in the creation of culture via the use of digital technology. However, as highlighted by Lessig, such re-engagement is stifled by current copyright laws that protect almost any use of copyrighted material without permission. Currently, copyright laws are simply ignored in many settings. Maybe the *SABAM* court should have considered the balance between the need to protect intellectual property holder rights and the creative interests designed to be protected in the original copyright protection laws. Current permutations of the law provide for little balance between these rights and instead place prohibitive restrictions upon the creative processes. The absence of balance requires service providers to police online traffic for violations based in physical world realities or potentially face significant consequences.

¶36 It is worth noting, as Professor Lessig highlights, that this is not a general call for the removal of copyright protections. Wholesale copyright infringement should always be prohibited. But creative sampling, remixing, and other fair use[106] or derivative works should not be defined as acts of piracy, as doing so places service providers in the unsustainable position of being required to determine and apply these copyright exceptions. The question, as always, is one of line drawing and balance. What percentage of a work can be used and still be called a sample? Law varies significantly from jurisdiction to jurisdiction on this score. In an online world essentially without boundaries, ISPs should not be tasked with determining violations of copyright law, as these are determinations that must be done on a case-by-case basis. But few if any of these fact-specific, legal determinations can be easily and cost-effectively built into a filtering algorithm.[107] Case-by-case determination requires people, courts, and a level of human judgment, which is why the law should not require ISPs to make such determinations or penalize them for failing to police copyright infringement activity of their users. There are simply too many variables requiring case-specific judgment calls that are expensive in terms of both money and time. These are not burdens for service providers to undertake on their own.

¶37 Furthermore, criminalizing service providers incentivizes them to police the activity of its users[108]—an outsourced policing burden that service providers will have to

---

[105] *See* Larry Lessig, *Laws that Choke Creativity*, TED Talk, (Mar. 2007), http://www.ted.com/talks/larry_lessig_says_the_law_is_strangling_creativity.html.

[106] Fair use is a legal concept that has evolved into statutory law in the U.S. Many countries don't have fair use provisions in law instead providing enumerated exceptions from the exclusive rights of the rights holder, usually termed fair dealings. For a further discussion, *see* Baird, *supra* note 73.

[107] "[I]t is highly unlikely that technology will completely eliminate the problem of deciding whether any particular use of copyrighted material is permitted, uses only public domain material, or is fair use." Alfred C. Yen, *Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and the First Amendment*, 88 GEO. L.J. 1833, 1853 n.119. (2000).

[108] By imposing liability upon one party for the infringing actions of another party, the doctrine of vicarious liability provides an incentive to police market relationships. *See* Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 261-62 (9th Cir. 1996). *See also*, Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 907 F. Supp. 1361, 1375 (N.D. Cal. 1995).

begrudgingly comply with by creating algorithms to filter content or face stiff criminal and/or civil penalties. Consider the April 2012 German case in which Google was ordered to install filtering software onto its YouTube service to prevent the uploading of copyrighted material.[109] In contrast, in May 2012 the French Tribunal de Grande Instance declared that YouTube had made adequate efforts to remove copyright protected programs without the installation of additional filters or mechanisms prior to the uploading of material.[110] In other words, the German court requires filtering prior to uploading material while the French court requires a responsive removal mechanism, similar to U.S. law. How can a service provider keep abreast of and be compliant with these various laws with any real level of certainty? A higher level of certainty must be required before we criminalize action/inaction on the part of service providers.

¶38 Even the higher level of specificity within U.S. law has not stopped individuals and industry participants from suing some service providers in U.S. courts.[111] For example, YouTube has developed an advanced content monitoring mechanism that allows rights holders to notify YouTube of the presence of content protected by copyright.[112] The system requires rights holders to deliver to YouTube reference files of content they claim to own and metadata describing that content.[113] This information is then used to identify content on YouTube allegedly infringing upon the rights of others. In reality, YouTube's policies and content management system are robust and effective in preventing and responding to take down requests. YouTube even claims to have "maintained a dedicated team of employees on call around the clock to assist copyright owners in removing unauthorized material."[114] In short, YouTube has undertaken a significant burden that is most likely above and beyond what is required under E.U. or U.S. law. Are we willing to ask for an even greater commitment from service providers? And if they fail to comply with the law, are we willing to criminalize their actions or lack thereof?

---

[109] *See* Angela Moscaritolo, *German Court Orders YouTube to Filter Content, Remove Videos*, PCMAG.COM (April 20, 2012), http://www.pcmag.com/article2/0,2817,2403348,00.asp.

[110] *See* Eric Pfanner, *French Court Sides with Google in YouTube Case*, N.Y TIMES (May 29, 2012), http://www.nytimes.com/2012/05/30/technology/french-court-sides-with-google-in-youtube-case.html?_r=1&pagewanted=print. *See also,* Ke Steven Wan, *Managing Peer-to-Peer Traffic with Digital Fingerprinting and Digital Watermarking*, 41 SW. U. L. REV. 331 (2012).

[111] *See e.g*., Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913 (2005) (determining defendant P2P file sharing companies Grokster and Streamcast (maker of Morpheus) could be sued for inducing copyright infringement for acts taken in the course of marketing file sharing software). *See also* Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 907 F. Supp. 1361 (N.D. Cal. 1995) (determining that operators of the individual servers are not directly liable because there are so many of them involved in the infringement, it is difficult for them to police their systems, and there is always a user who can be held liable but that contributory or vicarious infringement is a real consideration); Sega Enterprises Ltd. v. MAPHIA, 948 F.Supp. 923 (N.D. Cal. 1996) (determining that Sega had established a case of contributory copyright infringement); A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001) (holding that defendant, peer-to-peer (P2P) file-sharing service Napster, could be held liable for contributory infringement and vicarious infringement of the plaintiffs' copyrights); Perfect 10, Inc. v. Amazon.com, Inc., 487 F.3d 701 (9th Cir.2007) (holding Google's framing and hyperlinking as part of an image search engine constituted a fair use of Perfect 10's images because the use was highly transformative).

[112] *See* YouTube *Website FAQ, Content ID, Block, Monetize, or Track Viewing Metrics-It's Automated, and It's Free*, http://www.youtube.com/t/contentid (last visited June 24, 2012).

[113] *See id*.

[114] *Viacom Int'l Inc. v. YouTube, Inc*., 718 F. Supp. 2d 514, 519 (S.D.N.Y. 2010); *see also* Memorandum of Law in Support of Defendants' Motion for Summary Judgment, at 17, section 3 (citing Levine Declaration, ¶¶ 5-10, 12, 14, 17-19).

¶39 Most concerning to the users of YouTube, however, is the fact that the Content ID system used by YouTube is an automated system. Consequently, it lacks human judgment and discretion in determining applicable protections for the alleged copyright violator. Instead, the system blocks any and all use of identified copyrighted material.[115] The YouTube system makes sense: it is a cost effective mechanism to eliminate the risk of YouTube hosting illegal material. However, the system most likely over captures information and communications, is biased towards assertions of intellectual property rights holders, and uses little to no human intervention or determinations in the process.[116] This is troubling given many of the concerns raised by the *SABAM* court. Service providers faced with criminal and/or increasingly onerous civil sanctions must make risk assessments in the designing of their system that err on the side of over-capturing information to protect themselves from liability. This amounts to using the threat of criminal sanctions to coerce ISPs to become internet policing bodies, which should not be allowed under any circumstances.

V. THE NEED TO HAVE A MULTI-FACETED APPROACH TO WIDESPREAD INFRINGING ACTIVITIES

¶40 Given the broad and varied nature of online copyright infringement, it's worth considering whether combating piracy in the manner being proscribed is having an impact on reducing infringing activity. As Internet and communication regulators in the United Kingdom wrote in *'Site Blocking' to Reduce Internet Piracy,*[117] there has to be a "broader package of measures to tackle infringement."[118] I suggest this broader package include three key areas of reform to assist service providers: (1) technology cooperative initiatives, (2) strengthening and clarifying the law, and (3) creating a truly shared burden of protection.

A. Technology Cooperation

¶41 Site blocking provides a means to prevent some infringing activity. However, the addition of complementary administrative measures would strengthen the overall effectiveness of anti-infringement efforts. In the UK it has been argued by commentators and intellectual property advocates alike that the first step should be to allow websites to be served with notice-and-take-down requests, similar to the common practice in the United States.[119] Implementation of such a process would allow service providers to react in an expedient manner to the illegal activities of its users. It is hoped this system would provide an incentive for compliance on the part of the service providers as their failure to comply might result in sanctions, penalties and/or the loss of revenue from the shutting down of the offending website. In addition, a system such as the one used in the U.S. would allow the service provider to ensure over-capture issues are minimized as the system could easily accommodate an appeal process and provide protections and

[115] *See* YouTube, *supra* note 1113.
[116] *See id*.
[117] *See* Office of Communications (Ofcom), *supra* note 93.
[118] *Id*.
[119] *See* 17 U.S.C. § 512(c)(3)(A)(i-vi) (2006).

timeframes for the return of a user's lawful material. However, as mentioned above, the implementation, monitoring and associated costs of such a system should not be borne by the service providers alone. Intellectual property right holders should be expected to undertake some of the burden associated with such a system. The use of a notice-and-take-down system allows the burden of detection to be rightly placed upon the intellectual property rights holders. The rights holders should also bear some of the ever increasing costs associated with the take down requests as well.

¶42 Even in the face of notice-and-take-down mechanisms and website blocking efforts, users truly intent on circumventing intellectual property right protections will find a way to distribute and access content unlawfully. So any proposed measure must appreciate the need to block access to infringing websites or user content in a cost-effective and timely manner. Arguing that every blocking attempt must be accompanied by a court hearing misses the main point: the system must be responsive to immediate needs. If the online community is serious about reducing the copyright infringing activity of some of its users, implementation must be done quickly, since much of what constitutes infringing activity involves live "feeds"[120] and immediate access to pre-release movies and music. Without the ability to block such immediate activity, much of the potential benefit of blocking would be lost. Consequently, blocking websites via a temporary restraining order is currently the only real solution. However, the actions should be short-lived and must provide legal protections for service providers that comply with requests that turn out to be baseless.

¶43 When a website is blocked, the benefits are often short-lived as the operator of the website can easily re-establish it at a different IP address, URL, or domain,[121] and the new site can then be "re-found" through a simple search. Consequently, a system of protective measures must take into account search engines. In January 2012, the British Recorded Music Industry (BPI), Motion Pictures Association (MPA), Producers Alliance for Cinema and Television (PACT), The Premier League, and the Publishers Association proposed an "Anti-Piracy Code of Practice for Search Engines."[122] The proposed code requires search engines to relegate sites in their rankings for repeatedly making available pirated content. To facilitate such a change, search engines would be expected to promote within their rankings "licensed" or "certified" websites.[123] Search engines would also agree to stop promoting pirate websites, to not place ads on those sites, and refrain from selling keyword advertising related to piracy terminology.[124] Unsurprisingly, many of the largest search engines have taken issue with being forced to

---

[120] *See* U.S. Immigration and Customs Enforcement's News Release, *New York Investigators Seize 10 Websites That Illegally Streamed Copyrighted Sporting And Pay-Per-View Events* (Feb. 2, 2011), http://www.ice.gov/news/releases/1102/110202newyork.htm.

[121] There are reports that this is precisely what happened in the Megaupload situation, *see* BBC News, Technology Section, *New site Megabox from Megaupload's Kim Dotcom* (June 22, 2012), http://www.bbc.com/news/technology-18547814.

[122] Pinsent Masons LLP, *Anti-Piracy Code of Practice For Search Engines Proposed by Rights Holder Representatives* (Jan. 27, 2012), *available at* http://www.out-law.com/en/articles/2012/january-/anti-piracy-code-of-practice-for-search-engines-proposed-by-rights-holder-representatives/.

[123] *See* Open Rights Group, *Responsible Practices for Search Engines in Reducing Online Infringement Proposal for a Code of Practice, available at* http://www.openrightsgroup.org/assets/files/pdfs/proposals%20to%20search%20engines.pdf (last accessed Feb. 3, 2012).

[124] *See id.*

shoulder such heavy burdens instead of sharing the burden with rights holders.[125] And rightly so, as this is yet another example of conflict being created within an industry that could be a key component in creating the cooperation needed to achieve the goal of reducing online piracy. Neither party should bear the bulk of the burden; it should be a burden shared by all entities. However, the use of search engines as part of a broader package of technology-based mechanisms working cooperatively to reduce copyright infringement is a reasonable burden search providers must be encouraged to embrace. Cooperation amongst the technology providers is the only true long-term means of reducing online piracy.

B. Legal Strengthening and Clarification

¶44 As previously noted, the law is often unclear, poorly designed, and unreflective of current social norms. Without a doubt, copyright laws need to be reviewed[126] and most likely need, at a minimum, to be harmonized if not reimagined as part of a centralized system. Such reforms would allow service providers to fully appreciate legal risks on a global scale and to better protect their interests. Moreover, proper legal reform could remove some concerns relating to the need for ongoing court involvement and might provide protections for actions that service providers take to protect materials. Finally, many commentators argue that any reform of intellectual property protections should include a provision to prohibit circumvention of those protections.[127] Including such a provision would return some of the previous balance of enforcement to intellectual property right holders, who would be incentivized to improve protection and anti-circumvention technology. Unquestionably, the law should be careful in preventing the recording, motion picture and software industries from over-protecting their rights with the use of circumvention technology, as the industries should not be able to overly restrict its property via contract and legal proscriptions in the face of more open and flexible

[125] *See* Giulio Coraggio, *Google NOT Liable for Search Results*, IPT ITALY BLOG (June 13, 2012), http://blog.dlapiper.com/iptitaly/entry/google_not_liable_for_search (explaining the court determined that Google as a caching provider was obliged to remove infringing material only following a court order).

[126] *See e.g.*, Uma Suthersanen, *The First Global Copyright Act*, THE FIRST GLOBAL COPYRIGHT ACT, IN A SHIFTING EMPIRE: 100 YEARS OF THE COPYRIGHT ACT 1911 (U. Suthersanen & Y. Gendreau, eds.); Edward Elgar, (2012). *See also* Mireille Van Eechoud et al., *Harmonizing European Copyright Law: The Challenges of Better Lawmaking*, INFORMATION LAW SERIES 19 (May 2012); James Griffin, *300 Years of Copyright Law? A Not so Modest Proposal for Reform*, 28 J. MARSHALL J. COMPUTER & INFO. L. 1 (2010) (calling for an increased ability of content recipients to re-use works); Peter Menell, *Envisioning Copyright Law's Digital Future*, 46 N.Y.L. SCH. L. REV 63 (2002-03) (calling for a general transformation of copyright law from a property rights orientation toward a regulatory regime); Pamela Samuelson et al., *The Copyright Principles Project: Directions for Reform*, 25 BERKELEY TECH. L.J. 1176 (2010) (exploring improvements to be made in relation to U.S. copyright law); Peter Yu, *Digital Copyright and Confuzzling Rhetoric*, 13 VAND. J. ENT. TECH. L. 881 (2011) (examining what the industry could do to lessen copyright infringement).

[127] *See, e.g.*, Jeremy DeBeer, *Locks & Levies*, 84 DENV. U. L. REV. 143 (2006) (contrasting stakeholders preferences in the manner to protect online property); Ewa Davison and Steve Calandrillo, *The Dangers of the Digital Millennium Copyright Act: Much Ado about Nothing?*, 50 WM. & MARY L. REV. 349 (2008) (considering circumvention technology within the DMCA); Sylvia Kierkegaard, *Outlawing Circumvention of Technological Measures Going Overboard: Hollywood Style*, 22 COMPUTER L. & SEC. REP. 46 (2006) (considering whether the use of circumvention technology has gone beyond the original protections afforded to copyright holders); Emanuela Arezzo, *Videogames and Consoles Between Copyright and Technical Protection Measures* (June 26, 2008) *available at* SSRN: http://ssrn.com/abstract=1151654 (considering the distortional market impact that may be created based on its use).

copyright laws.[128] But a well-crafted legal reform would appreciate each of these attributes and needs and could be crafted precisely as the *SABAM* court most likely intended, with an eye toward balancing the needs and rights of all the parties involved within the online community.

C. A Truly Shared Burden

¶45 Finally, I would like to emphasize an important actor often forgotten when discussing online intellectual property right infringing activity: individual users. People who use the Internet have a vested interest in protecting its usefulness, openness and inexpensive availability. To ensure these attributes are protected the entire online community must become involved in a level of self-policing or face the likely reality of legislative proscriptions that will impact and most likely curtail freedoms enjoyed by Internet users. Yet few entities highlight the real possibility that individuals may provide an appropriate avenue of reducing infringing activity[129] by increasing their negative attitude toward copyright infringement.[130]

¶46 Currently, the burden of reducing infringing activity online is shared primarily by right holders and service providers. Placing the burden primarily on these two entities creates a strange and conflicted online world, in which commercial entities stand in the most powerful position when it comes to creating the mechanisms to police it. This is not a situation the online community should accept, as it will create a system of intellectual property protections based on economics instead of fairness, due process and freedom.

¶47 Systems created by right holders and/or service providers will likely be more restrictive than the law requires, as both parties need to protect their economic interest. For example, consider the business profile of Virgin Media primarily located in Europe. Virgin Media has an interest as both an intellectual property rights holder and a service provider. It is not difficult to imagine a monitoring and removal system designed to protect both of these interests at the expense of Internet communications freedom.[131] At least one potential example of this dilemma already exists, the previously discussed Content ID system used by YouTube. The YouTube system technically complies with the counter-suit requirements of the U.S. Digital Millennium Copyright Act (DMCA) but does so in a very inefficient manner and provides little redress for lawful users wrongfully accused of copyright infringement. Such a system gives right holders substantial control of online content available on the YouTube platform. In this situation, the liability of the system provider holds a more important position in terms of risk assessment—as a rights holder (or an entire industry) is more likely to pursue an action

---

[128] S*ee* Dan Burk, *Legal and Technical Standards in Digital Rights Management Technology*, MINN. LEGAL STUD. RES. PAPER No. 05-16 (April 5, 2005) *available at* http://ssrn.com/abstract=699384 (discussing the potential benefits and pitfalls of the use of technology as a copyright protector).

[129] In fact, as highlighted in a 2009 research into young people's attitudes toward copyright infringement: "These young people (participating in the survey) speak of a sense of who ought to be responsible for the illegal activity—either the online intermediary or the government—while resisting the sense that they might also bear some responsibility in these scenarios." *See* Palfrey, *Youth, Creativity, and Copyright*, *supra* note 71.

[130] *See* Mark Schultz, *Fear and Norms and Rock & Roll: What Jambands Can Teach Us About Persuading People to Obey Copyright Law*, 21 BERKELY TECH. L.J. 651 (2006).

[131] *See* Wendy Seltzer, *Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment*, 24 HARV. J.L. & TECH. 171 (2010).

against the service provider in court. In these situations, forgotten are the vast majority of online users lawfully uploading content and voluntarily complying with copyright protections. Within this system the lawful online users are given no real means to challenge the removal or blocking of lawful information as they simply lack resources, initiative or legal protections to pursue actions against service providers as individuals. Therefore, in addition to calling for a multi-faceted approach to protecting rights holders with the cooperation of service providers, it is time to engage lawful Internet users in the protection process or the economic interests of businesses and the interests of rights holders will be given prominence in creating the system of intellectual property right protections in the online world. Individuals must begin to do their part and ensure they are considered within the balance equation. Such is the balance that courts should demand, by spreading the responsibility of ending infringing activities in the online world across the entire community.

VI. CONCLUSION

¶48 The *Newzbin* cases mark a clear shift in the responsibility that European entities must take to protect intellectual property rights. Previously, the burden of protecting intellectual property rights fell primarily on rights holders. Today, however, legislative bodies and courts, in both the E.U. and the U.S., have shifted this expectation of protections to a shared burden amongst service providers and rights holders. However, *SABAM* created a cooperative burden to protect intellectual property rights that lacks legal proscription and is therefore opening service providers to increased legal uncertainty. While the *SABAM* court did limit the burden that service providers can be expected to undertake to a specific, targeted, and precise injunction requiring the use of existing technology, the court has not gone far enough to consider the total burden being placed on service providers. The use of fundamental balances, overly burdensome proscriptions, ongoing court intervention, and criminalization of users and service providers will not provide a lasting impact in reducing online piracy nor will it reduce service providers' fears of litigation. Instead, a multifaceted approach must be crafted that recognizes and places corresponding burdens on the entire community: rights holders, service providers, and regular Internet users. To accomplish this balance, several things must occur: (1) industry and service providers must work together to establish technology cooperative initiatives, (2) the law must be crafted in a manner that recognizes current online realities and be drafted as regulatory in nature, with an eye toward cooperation instead of conflict and over-penalization, and (3) the entire online community must recognize a shared burden of intellectual property protections. This is the balance that the next court must seek to achieve.