Northwestern Journal of Technology and Intellectual Property

Volume 11 | Issue 6 Article 1

2013

Heavyweight Bots in the Clouds: The Wrong Incentives and Poorly Crafted Balances That Lead to the Blocking of Information Online

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

Heavyweight Bots in the Clouds: The Wrong Incentives and Poorly Crafted Balances That Lead to the Blocking of Information Online

Anjanette H. Raymond

August 2013 VOL. 11, NO. 6

Northwestern Journal of Technology and Intellectual Property
Volume 11, Number 6 (August 2013)

Heavyweight Bots in the Clouds: The Wrong Incentives and Poorly Crafted Balances That Lead to the Blocking of Information Online

By Anjanette H. Raymond*

The United States and the European Union have long recognized the need to protect ISPs from potential liability from customers using their services to infringe intellectual property rights. These protections arise from a long-standing belief that intellectual property right holders should bear the burden of protecting their property, even in the quick moving Internet environment. However, a recent series of cases has called into question the ISPs' liability protections as their technology is often the only real means to prevent wide scale infringing activity. This series has caused courts to revisit ISPs' liability and to impose a 'cooperative burden' requiring ISPs to assist in the protection of intellectual property rights. In creating this burden, the ISPs and right holders have reacted by working together to craft technology advances that identify infringing activities. However, the technology is not yet ready for wide scale use and is often accompanied by policies that encourage the over-identification of material that should never be considered infringing. The over-identification is even more troubling in the face of automatic blocking activities that allow entities to claim material that is not part of their intellectual property portfolio. This activity is preventing communication, blocking the dissemination of information, and sometimes holding rightful owners of the material hostage to the automatic bot shut down activities. Simply put, this new cooperative burden is creating an odd set of incentives with no regard for individual internet users' rights.

This paper will consider incentives created under the law for ISPs to over-protect intellectual property rights. The paper will then consider the creation of an appropriate balance between stakeholders within the online world—one that re-evaluates the priority given to right holders and instead truly balances the burden of protecting intellectual property in the online world. Finally, the paper will suggest that the law must be reconsidered in light of the new technologies being employed by ISPs and intellectual property right holders in an effort to combat online piracy at the expense of individual users.

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

I. INTRODUCTION

¶1 On August 6, 2012, NASA broadcasted online one of the scientific, technological, and educational highlights of the decade when it live streamed the landing of its Mars rover Curiosity. Curiosity had traveled hundreds of millions of miles through space to explore the red planet.[1] The online broadcast marked the first time that such a stunning display of the red planet had been seen live by millions of interested parties worldwide. With technology and human know-how on worldwide display, the achievement was simply remarkable. But unfortunately, another technology—one a little closer to home—would, in the end, grab the headlines, as online video highlights of the landing would be blocked from public view for copyright reasons.

¶2 NASA has long hosted a video stream featuring video highlights and educational programs on various NASA-related projects. No one could have anticipated that the posting of the Curiosity landing on NASA's YouTube channel would cause any trouble or controversy.[2] But soon after NASA posted the thirteen-minute excerpt, the video was blocked by YouTube copyright technology.[3] Despite the fact that NASA produced the

[1] *See* Elizabeth Landau, *Mars Landing Went 'Flawlessly,' Scientists Say*, CNN (Aug. 14, 2012), http://edition.cnn.com/2012/08/06/tech/mars-rover-curiosity/index.html.

[2] The NASA television channel is available at http://www.youtube.com/nasatelevision.

[3] *See* Timothy B. Lee, *As Curiosity Touches Down on Mars, Video Is Taken Down from YouTube*, ARS TECHNICA (Aug. 6, 2012), http://arstechnica.com/tech-policy/2012/08/as-curiosity-touches-down-on-mars-video-is-taken-down-from-youtube/.

video and had every right to broadcast it online, the video activated a warning within the YouTube copyright identification system resulting in the video being blocked for "copyright reasons." As MotherBoard author Alex Pasternack noted:

> [A] NASA-made public domain video posted on NASA's official YouTube channel, documenting the landing of a $2.5 billion Mars rover mission paid for with public taxpayer money, was blocked by YouTube because of a copyright claim by a private news service.[4]

YouTube shortly restored the video, but the irony was clear. The video had been identified and disabled via the use of an automated identification technology employed within the YouTube system. In fact, the NASA video was blocked again a few days later when a commentator used a series of splashes from the video to highlight his discussion about the landing.[5] This particular blocking occurred despite NASA notifying the technology manager that the video was within the public domain and should never be blocked.

¶3 As emphasized by NASA spokesperson Bob Jacobs and highlighted by Parker Higgins:

> We spend too much time going through the administrative process to clear videos slapped with needless copyright claims. . . . YouTube seems to be missing a 'common sense' button to its processes, especially when it involves public domain material paid for by the American taxpayer.[6]

Technology is being employed to assist copyright holders and service providers in identifying and blocking media identified as copyright infringing material. Yet the technology is over-identifying and over-blocking media that should not be blocked, and as demonstrated by the NASA YouTube video, it seems that there is little to no human oversight.

¶4 Because the Mars landing was an after-the-fact video that was quickly restored after being blocked, we may assume that this is a limited example. Unfortunately, it is not. In fact, media blocking occurs even when the event is live or is displaying a video demanding immediate release, such as a political rally or social commentary. For example, videos from both the Hugo Science Fiction Award ceremony and the Democratic National Convention were disabled as a result of the implementation of similar digital fingerprinting technology.[7] The Hugo Science Fiction Award ceremony is

---

[4] Alex Pasternack, *NASA's Mars Rover Crashed into a DMCA Takedown*, VICE MAGAZINE MOTHERBOARD (Aug. 6, 2012), http://motherboard.vice.com/2012/8/6/nasa-s-mars-rover-crashed-into-a-dmca-takedown.

[5] *See* Timothy B. Lee, *How YouTube Lets Content Companies "Claim" NASA Mars Videos*, ARS TECHNICA (Aug. 8, 2012), http://arstechnica.com/tech-policy/2012/08/how-youtube-lets-content-companies-claim-nasa-mars videos/.

[6] Parker Higgins, *Mars Landing Videos, and Other Casualties of the Robot Wars*, ELECTRONIC FRONTIER FOUNDATION (Aug. 8, 2012), https://www.eff.org/deeplinks/2012/08/mars-landing-videos-and-other-casualties-robot-wars.

[7] S*ee* Annalee Newitz, *How Copyright Enforcement Robots Killed the Hugo Awards*, I09 (Sept. 3, 2012, 10:25 AM), http://io9.com/5940036/how-copyright-enforcement-robots-killed-the-hugo-awards; Ryan Singel, *YouTube Flags Democrats' Convention Video on Copyright Grounds*, WIRED (Sept. 5, 2012, 12:10 AM), http://www.wired.com/threatlevel/2012/09/youtube-flags-democrats-convention-video-on-copyright-

a prestigious award ceremony for science fiction.[8] One of the main ways that Sci-Fi fans watch the awards is through the use of the streaming service Ustream,[9] which broadcasts the ceremony live. This year, during Neil Gaiman's acceptance speech for his *Doctor Who* script, "The Doctor's Wife," the video stream was blocked and replaced with the message "Worldcon banned due to copyright infringement."[10] Unsurprisingly, the award ceremony had shown video clips of portions of "The Doctor's Wife" as a lead-in to the speech. These video clips—ones provided by the studio and fully authorized to be used in the ceremony—had set off the digital restriction management technology employed by Ustream.[11] The fully authorized use of a video had shut down the online streaming video of one of the most prestigious Science Fiction Awards and had done so during an award for *Doctor Who*. Even worse, the award ceremony video could not be restored, so the public was blocked from seeing the ceremony.[12]

¶5 Even more concerning are events surrounding the blocking of the live stream of the 2012 Democratic National Convention.[13] On September 4, 2012, the DNC posted on YouTube, an official streaming partner, several videos of speeches and other highlights of the DNC's evening events, all of which were featured prominently on BarackObama.com and the YouTube channel DemConvention2012. Some portion of the DNC video triggered the YouTube digital fingerprinting system, and as a result, YouTube put a copyright blocking message on the livestream video. The message that appeared instead of the video is clear:

> This video contains content from WMG, SME, Associated Press (AP), UMG, Dow Jones, New York Times Digital, The Harry Fox Agency, Inc. (HFA), Warner Chappell, UMPG Publishing and EMI Music Publishing, one or more of whom have blocked it in your country on copyright grounds. Sorry about that.[14]

The notice indicates that numerous agencies and publishing groups are potentially claiming copyright concerning a video that the DNC created and clearly had rights to broadcast and rebroadcast. The ability of non-holders of copyrighted material to claim video as part of an intellectual property rights portfolio is possibly the most concerning use of digital fingerprinting technology. As Wired magazine author Andy Baio explains:

---

grounds/.

[8] *See* Newitz, *supra* note 7; Will Oremus, *Sci-Fi Awards Webcast Shut Down by Rogue Copyright Bots That Refuse To Obey Human Commands*, SLATE (Sept. 4, 2012, 4:21 PM), http://www.slate.com/blogs/future_tense/2012/09/04/hugo_awards_ustream_science_fiction_webcast_blocked_by_rogue_copyright_bots.html; Zachary Knight, *Copyright Enforcement Bots Seek And Destroy Hugo Awards*, TECHDIRT (Sept. 4, 2012), http://www.techdirt.com/articles/20120903/18505820259/copyright-enforcement-bots-seek-destroy-hugo-awards.shtml.

[9] The Ustream service is a 'broadcast yourself' service, similar to YouTube. It is available at http://www.ustream.tv/new.

[10] *See* Newitz, *supra* note 7.

[11] *Id*.

[12] At the time, Ustream used Vobile, a third-party service that does automated infringement takedowns. Shortly after the ceremony, Ustream claimed it could not restart its own live feed once Vobile had shut it down. Knight, *supra* note 9.

[13] *See* Singel, *supra* note 7; Geeta Dayal, *The Algorithmic Copyright Cops: Streaming Video's Robotic Overlords*, WIRED (Sept. 6, 2012, 6:00 AM) http://www.wired.com/threatlevel/2012/09/streaming-videos-robotic-overlords-algorithmic-copyright-cops.

[14] *See* Singel, *supra* note 7.

> [T]here has been a dramatic rise in Content ID abuse in the past couple of years, wielded in ways never intended. Scammers are using Content ID to steal ad revenue from YouTube video creators en masse, with some companies claiming content they don't own deliberately or not. The inability to understand context and parody regularly leads to "fair use" videos getting blocked, muted or monetized.[15]

¶6 Based on the incidents I've described above, it is clear that automated enforcement technology is not yet ready for widespread implementation. As technology expert Parker Higgins notes: "It's impossibly complicated to define in a set of 'business rules' for automated [copyright] enforcement."[16]

¶7 But while the implementation of digital fingerprinting and similar technology is problematic, it is even more problematic that service providers are allowing and even encouraging its use. Historically, service providers have protected online users from such troubling and problematic technology. However, recent court cases have created a new online world where service providers are expected to cooperate in preventing copyright infringement. As a result, service providers have begun to implement technology to cooperate in the effort to prevent online piracy. Copyright holders and service providers have gone a step further and have created policy surrounding the technology that results in money being made from blocking. The new cooperative relationship between service providers and copyright holders should be very troubling for online users.

¶8 This paper will consider incentives created under the law for service providers to over-protect intellectual property rights. The paper will then consider the creation of an appropriate balance between stakeholders within the online world—one that re-evaluates the priority given to right holders and instead truly balances the burden of protecting intellectual property in the online world. Finally, the paper will suggest that the law must be reconsidered in light of the new technologies being employed by ISPs and intellectual property right holders in an effort to combat online piracy yet at the expense of individual users.

II. A BIT OF BACKGROUND AND STAGE SETTING

¶9 To fully understand the difficulties arising from the growing use of digital fingerprinting technology, a brief examination of the technology is necessary. Digital fingerprinting technology is software created to identify a piece of media and relate it to an external database.[17] The software samples an audio or video file and identifies minute portions of the file unique to that piece of media.[18] It then compares the identified sample to an external database of other unique pieces of media.[19] The more matches occurring between the two pieces of media, the more likely the media files are one in the same. Some digital fingerprinting technology service providers claim to be able to accurately

---

[15] Andy Baio, *Copyright Kings Are Judge, Jury and Executioner on YouTube*, WIRED (Feb. 2, 2012, 1:29 PM), http://www.wired.com/business/2012/02/opinion-baiodmcayoutube.

[16] Higgins, *supra* note 6.

[17] *See* Wesley Fenlon, *How Digital Fingerprinting Works*, HOW STUFF WORKS, http://computer.howstuffworks.com/digital-fingerprinting2.htm (last visited Feb. 10, 2013).

[18] *See id.*

[19] *See id.*

identify "across file formats, codecs, bitrates, and compression techniques"[20] even when transformations "such as transcoding, downmixing, equalization, injected noise, timescaling, framedrops, grayscaling, cropping, image shifting, contrast and brightness adjustments, blurring, camcordering"[21] have been used to create or alter the media. If these claims are even partially true, digital fingerprinting technology is a serious software development in the fight against online piracy, as it not only identifies identical or similar files but is also capable of disregarding alterations of files in the matching process.

¶10 Problems arise, however, with the policies and cost saving measures used for the mass rollout of this technology. Many systems allow individual users and owners to upload and tag files. As such, individuals are able to claim ownership and create identifiers used to flag the media. The issue with this type of system is immediately apparent as individuals, without any oversight, are allowed to identify material that may or may not truly belong within his intellectual property right portfolio. Consider 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.[22]

¶11 As a result, ISPs are being inundated with takedown requests, some legitimate and others disreputable attempts to restrict the use of material that is not part of the individuals portfolio. In both instances, as well as numerous others, the material should not be removed or blocked, yet the system as designed fails to weed out these attempts to over-claim non-existent rights. Even more troubling are those digital fingerprinting providers that allow individuals to create a response to identified media that the system will follow, without challenge. For example, within some digital fingerprinting systems, alleged intellectual right holders are allowed to create a response to an identified media that blocks or monetizes the video.[23] Monetization allows the right holder to elect to

---

[20] *Audible Magic Technology Overview*, AUDIBLE MAGIC, http://audiblemagic.com/technology.php (last visited Sept. 14, 2012).

[21] *Id*.

[22] Letter from Sarah B. Deutsch, Vice President and Associate General Counsel Verizon Communications Inc. to Copyright Office, Library of Congress, Request for Public Comment on Designation of Agent to Receive Notification of Claimed Infringement (Nov. 28, 2011), 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) (discussing the use of digital technology as a management device).

[23] For example, YouTube allows the selection of monetization as a response to the posting of a potentially infringing video or audio file. *See YouTube Policy, Content ID, Block, Monetize, or Track Viewing Metrics — It's Automated, and It's Free*, YOUTUBE, http://www.youtube.com/t/contentid (last viewed Feb. 10, 2013).

allow the copyright infringing video to play with the response to identification being the addition of direct advertising.[24] One can quickly appreciate how this system is ripe for abuse because there is little oversight of the digital identification system. Similarly, money can be made from improperly claiming and monetizing intellectual property that is not actually within the individual's (or studio's) portfolio.

¶12 Blocking policies also raise concerns when accompanied by little oversight. Consider the situation that occurred with NASA and the technology that blocked their video. This blocking occurred with no check and balance, no oversight, and little recourse other than NASA requesting the video be re-posted. Now, consider the same set of circumstances with a small change. It is not a NASA video that is blocked, but an important social event such as the Democratic National Convention or the direct videos of police over-reactive response to an uprising. Because digital fingerprinting technology relies upon individuals to upload and claim ownership of video and similar media without any real oversight,[25] individuals can improperly claim ownership of media. If the true owner fails to tag the video within the system, an unscrupulous individual or entity can seize upon that mistake and improperly claim ownership of the video, effectively denying the broadcasting of the video. Even more concerning is the resolution of conflicts in the system,[26] again done with no real oversight. In this situation, the true owner could tag the video as part of their intellectual property portfolio, but an unscrupulous entity can also claim ownership. Although the second party has no ownership, the individual has been able to create a conflict within the system: that of contested ownership. In these situations the video is blocked until the issue can be resolved,[27] effectively shutting down the video from broadcast. Sinister claims, yet the current unmonitored system seems to allow for the possibility of such occurrences. And finally, consider a very real situation involving local bands and video producers that appropriately license the performance of material or catalogues. It is easy to imagine a local cover band playing a licensed performance of a currently popular song and then posting a video on YouTube or Facebook.[28] Is this video also to be blocked? While you might assume the answer has to be a resounding "YES!" this is not necessarily the case because it depends on the law at the place of performance, the place of viewing, the place of posting, and of course, the actual license agreement that might have allowed this original performance.[29] The band

[24] YouTube even has a YouTube Channel explaining the use of monetization. *See Topic - Monetization*, YOUTUBE, http://www.youtube.com/channel/HCXXD5Hq6CrX0 (last visited Feb. 10, 2013).

[25] *See Audible Magic Technology Overview*, *supra* note 20.

[26] *See id.*

[27] *See id.*

[28] *See* Mark F. Schultz, *Fear and Norms and Rock & Roll: What Jambands Can Teach Us About Persuading People to Obey Copyright Law*, 21 BERKELEY TECH. L.J. 651 (2006) (exploring pro-copyright social norms and the jamband community). In fact, several websites list bands that encourage their fans to perform the band's music and post a video of the recording online. *See* Bands That Allow Taping, http://btat.wagnerone.com (last visited Feb. 13, 2013); *Trade Friendly*, ETREE, http://wiki.etree.org/index.php?page=TradeFriendly (last visited Feb. 13, 2013).

[29] The full parameters of the law are much too large for coverage within this article. For more information see generally AM. SOC'Y OF COMPOSERS, AUTHORS AND PUBLISHERS, http://www.ascap.com/licensing/termsdefined.html (last visited Feb. 13, 2013); Giuseppe Mazziotti, *New Licensing Models for Online Music Services in the European Union: From Collective to Customized Management* (Columbia Public Law Research Paper No. 11-269, 2011), *available at* http://ssrn.com/abstract=1814264 (examining the restructuring of online rights management within the European Union).

may have had performance rights, including the right to rebroadcast their rendition of the popular song. However, this information is known to the band, the entity that licensed the playing of the song, and few others. Certainly the technology does not have this information and has no mechanism to gather such information.[30] As a consequence, a local band playing and broadcasting a fully authorized rendition of the song may see their video blocked. Why? Simple. The original widely recognized band playing their rendition of the song will have tagged their song within the system. In this situation, the system may not be able to distinguish between the two different renditions of the same song and may identify the authorized local performance as an infringing activity. Without a level of oversight, this video will be blocked, as will all videos that use small snippets of songs and similar media well authorized within the fair use doctrine. An automated system cannot make these nuanced legal determinations and as a result will over-block media. It is easy to see why the current system seems to be unready for wide scale adoption because there is no real means to untangle these highly important determinations without a significant level of context-based decision making.

¶13 One should not be surprised, however, that digital identification providers have created a system that maximizes the persistence, attention, and time commitment of intellectual property right holders attempting to protect their rights from online piracy. The current system is really a win-win scenario for fingerprinting technology providers and right holders. Digital fingerprinting technology providers use the resources and time of intellectual property right holders to upload millions of files, create billions of identifiers, and create a very large database of information. Technology providers' costs arise from designing and maintaining the functionality of the software and are passed on to the intellectual property right holders when they elect to use the service. The burden of data entry and maintenance costs of the database are passed on to the right holders, the cost of shut down is passed on to the ISPs or intermediaries, and the software development company maintains the system but charges the right holders for the ongoing use of the software.

III. STRANGE INCENTIVES IN THE CURRENT ONLINE ENVIRONMENT

¶14 It is important to recognize the existence of three key stakeholders in the online piracy debate: (1) intellectual property right holders; (2) Internet service providers and intermediaries; and (3) online users. Each of these stakeholders is protected in various ways, under various laws, on a global scale. In the majority of instances the law seeks to create a balance between the three stakeholders. However, the current online environment, coupled with sometimes outdated existing law, has shifted the balance among these three stakeholders in a substantial way. This balance shift stems from three sources: (1) laws that protect ISPs, which were written at a time when the online world was less efficient; (2) technology advances that make the online environment much faster, smoother, and barrier-free; and (3) growing concern that intellectual property rights are being infringed sometimes on a massive scale. To examine the convergence and impact of these issues, this section will examine the law, incentives, and

[30] *See Audible Magic Technology Overview*, *supra* note 20.

consequences of each in relation to individual users in both the European Union and the United States.

A. The European Stage of Considerations

¶15 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.[31] Numerous European Union directives exist along these lines. In the United States, the Digital Millennium Copyright Act[32] provides various and more specific protections to ISPs. In both instances, the 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.[33] However, many of these laws are also allowing ISPs to ignore or turn a blind eye to the infringing activities of their users.

---

[31] 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. & STRATEGIES 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'Y 389, (2004) (exploring virtual property); Lucille M. 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 M. Urban, *Protecting Open Innovation: The Defensive Patent License as 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) *available at* 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 (Nov. 28, 2011), http://articles.cnn.com/2011-11-28/tech/tech_websites-counterfiet-goods_1_counterfeit-goods-phony-goods-websites?_s=PM:TECH.

[32] *See generally* Orin Kerr, *A Lukewarm Defense of the Digital Millennium Copyright Act*, *in* COPY FIGHTS: THE FUTURE OF INTELLECTUAL PROPERTY IN THE INFORMATION AGE (Adam Thierer and Wayne Crews eds. 2002) (arguing for the realization that there is a logic to the organization and approaches contained within the DMCA); Bill Herman and Oscar 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 589 (2009) (exploring caches under the DMCA); Michael S. Sawyer, *Filters, Fair Use & Feedback: User-Generated Content Principles and the DMCA*, 24 BERKLEY TECH. L.J. 363 (2009) (exploring user generated content liabilities under the DMCA); Phil Weiser and Gideon Parchomovsky, *Beyond Fair Use*, 96 CORNELL L. REV. 91 (2011) (examining fair use under the DMCA).

[33] *See* Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, 200 O.J. (L 178) 12-15. [hereinafter E-Commerce Directive]. For a full comparison of the EU laws and the DMCA, see generally Miquel Peguera, *The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems*, 32 COLUM. J.L. & ARTS 481 (2009) (examining the similarities and differences between the two legal regimes).

¶16 In England, the 2010 cases of *Twentieth Century Fox Film Corp and Others v. Newzbin Ltd*[34] and *Twentieth Century Fox Film Corp and Others v. British Telecommunications*[35] presented a real tipping point after which it was clear that service providers had to become cooperative partners in the prevention of online piracy. The *Newzbin* case[36] serves as a perfect example of the difficulties intellectual property right holders face when attempting to prevent illegal downloading of material. Newzbin was a content aggregator site that allowed users to search the Internet for locations of a specific type of file (NZB). Similar to a torrent,[37] NZB files do not contain the file itself, but rather, contain 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 or files can be downloaded and viewed. The use of torrents and similar types of files has long been viewed as a clever way for a website to claim that it is not infringing copyrights because the website is doing nothing more than providing links. The film studios argued that the Newzbin site was "focused on piracy in that it locates and categorises unlawful copies of films and displays the titles of these copies in its indices; provides a facility for its users to search for particular unlawful copies and displays the results; and provides a simple one-click mechanism whereby users can acquire unlawful copies of their choice."[38] The High Court in London agreed, determining that Newzbin was "liable to the claimants for infringement of their copyrights,"[39] and in March 2010, the court ordered an injunction to restrain Newzbin "from infringing the claimants' copyrights in relation to their repertoire of films."[40] 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. Almost unsurprisingly, the website hosts launched a new, yet identical, website a short time later, even calling the new website a similar name,[41] but this time outside the reach of the United Kingdom courts. Newzbin2, as the new site was known, would be available to promote widespread copyright infringement. This case demonstrated to the world that website hosts could easily avoid court shutdown orders by merely shifting location. These shifts were so easy to accomplish that intellectual property right holders were left chasing the websites from jurisdiction to jurisdiction, with little hope of ever getting ahead of the game. To most, the problem was clear: copyright-infringing activity was widespread and the courts were limited by national boundaries. The existence of regulatory and enforcement boundaries within the physical

[34] [2010] EWHC 608 (Ch) (Eng.) [hereinafter *Newzbin*].

[35] [2011] EWHC 1981 (Ch) (Eng.) [hereinafter *Newzbin2*].

[36] *See generally* Anjanette H. Raymond, *Intermediaries' Precarious Balance Within Europe: Oddly Placed Cooperative Burdens in the Online World*, 11 NW. J. TECH. & INTELL. PROP. 359 (2013).

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

[38] *Newzbin* ¶ 1.

[39] *Id.* ¶ 126.

[40] *Id.* ¶ 135.

[41] The Newzbin 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 that 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' at the 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).

world was causing practical issues that left little choice but to ask the boundaryless ISPs and intermediaries to become cooperative partners with the intellectual property right holders in the prevention of online piracy. But how should this cooperative burden be undertaken and what share of the burden should fall upon ISPs and intermediaries?

¶17 The November 2011 case of *SABAM v. Scarlet Extended*[42] provides a perfect example of the dilemma of online piracy and the balance that must be struck between the rights of all in the online world. In 2004, SABAM[43] discovered that subscribers to the Belgian ISP Scarlet Extended (Scarlet) were using the ISP's services to illegally download, through peer-to-peer (P2P) networks, protected works from its catalogue, without authorization and without paying royalties.[44] SABAM thus requested that a Belgian Court issue an injunction against Scarlet forcing it to block any downloading or uploading of illegal files via P2P networks without authorization.[45] In June 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.[46] 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 enshrined within EU law.[47] The Brussels Appeal Court proceeded to ask the European Court of Justice (ECJ) whether EU law 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.[48] In responding to the question, the ECJ went to great lengths to consider the potential conflict between several EU Directives concerning information, intermediaries, copyright rights holders,[49] and the European Convention on the Protection of Human Rights and Fundamental Freedoms, specifically the protection of copyright and the protection of the fundamental rights of individuals.[50] In making its determination, the *SABAM* court recognized two fundamental issues in relation to service providers. First, the court affirmed existing EU case law and academic commentary placing service providers in a position to cooperate with intellectual property rights holders in protecting copyright in the online world. Second, it

---

[42] Case C-70/10, 2011 E.C.R., *available at* http://curia.europa.eu/juris/document/document.jsf;?docid=115202&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=132783 [hereinafter *SABAM*].

[43] One should note I have had to rely upon *SABAM* and *Newzbin2* for the basic summary. *See SABAM*, *supra* note 42, ¶¶ 15–28 and *Newzbin2*, *supra* note 35, ¶¶ 165–77.

[44] *See SABAM*, *supra* note 42, ¶ 17.

[45] *See id.*

[46] *See id.* ¶ 21.

[47] *See id.* ¶ 28. See *infra* note 49, for the Directives comprising EU Law.

[48] *See SABAM*, *supra* note 42, ¶ 28.

[49] *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 195) 16; Directive 95/46 of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 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, 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, 2002 O.J. (L 201) 37.

[50] *See* 2011 Y.B. EUR. CONV. ON H.R. (Eur. Comm'n of H.R.) 8, 10.

began to establish the balance that must be maintained between a service provider's rights and intellectual property holder's rights. Concerning individuals, the court highlighted two additional areas of consideration in the creation of the prescribed balance: (1) the individual's right to the protection of his/her personal data, and (2) the individual's freedom to receive or impart information.[51]

¶18 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."[52] Fortunately, the court recognized the need to be more proscriptive in such an evolving area of law and proceeded to focus on three fundamental rights within the European Union that must be considered in creating the balance: (1) the right of business to conduct its business,[53] (2) the right of an individual to protect personal data,[54] and (3) the right of an individual to receive and impart information.[55] And because the weight of each set of rights shifts on a case-by-case basis, one can imagine a scale shifting the balance based on the specific facts of the circumstances presented.

¶19 Concerning the burden that an Internet service provider[56] must undertake to cooperate in the protections, European domestic 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 their customers' behavior within the EU.[57] Even in a situation where monitoring activities become less costly,[58] 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

---

[51] *See* Charter of Fundamental Rights of the European Union arts. 8, 11, Dec. 7, 2000 (2000 O.J. (C. 364)) [hereinafter Charter].

[52] *SABAM*, *supra* note 42, at ¶ 44.

[53] *See id*. at ¶ 46, *citing* Charter, *supra* note 51 at art.16.

[54] *See* Charter, art. 8 ("Everyone has the right to the protection of personal data concerning him or her"), art. 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.").

[55] 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." *See* E-COMMERCE DIRECTIVE, *supra* note 33.

[56] Other courts have considered a different balance. For example, in the US, Judge Posner used a cost-and-benefit analysis when considering the service providers 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: "if the filtering cost is not 'disproportionately costly as compared with the infringement averted,' ISPs should be required to filter." *In re* Aimster Copyright Litigation, 334 F.3d 643 (7th Cir. 2003).

[57] 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 violate this general monitoring provision. *See* L'Oreal SA & Ors, [2010] EWCA (Civ) 535 (Eng.) at 17 *citing* Directive 2004/48, art. 3 § 2, *supra* note 49.

[58] 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 "ISP to carry out general monitoring, something which is prohibited by Article 15(1) of Directive 2000/31." *SABAM*, *supra* note 42, at ¶ 40.

should bear: cost of implementation,[59] cost associated with upkeep, cost associated with monitoring,[60] level of data inspection required,[61] complexity of the system to be installed,[62] duration of the request,[63] and the technical feasibility of such a request.[64] Internet service providers cannot be asked to implement a system that monitors all information[65] for an unlimited time[66] at the exclusive cost of the ISP. [67] Such a general order would place an undue burden on service providers that constitutes a significant barrier to the service provider's core business. [68] However, according to the court, a specific, targeted, and precise injunction requiring the use of an existing technology to monitor behavior is a reasonable burden.[69]

¶20 But imagine a more wide-scale implementation of the digital fingerprinting technology system that places the majority of the burden on the intellectual property right holders. In this situation, there can be little argument for an undue burden being placed on the ISP. In fact, there may be little to no burden on its business. And while one could argue that the implementation of such a system is not in the best interest of ISPs, intermediaries, and website hosts as it will undoubtedly impact the number of subscribers to the service, one has to appreciate the realities of a shared-cooperative burden to protect intellectual property rights online. While the requested activity cannot unduly burden the business, digital fingerprinting technology: (1) places the creation and upkeep costs upon the right holder; (2) places implementation costs on the right holder; (3) places costs associated with the creation and upkeep of the database on the right holder; (4) places few costs upon the service provider as the technology blocks access and there is no legal requirement to monitor such activity; (5) requires a low level of data inspection; (6) is part of a fairly straight forward, uncomplicated system; and (7) is technically feasible. In this situation it is almost impossible to argue that an undue burden on the service provider exists. Additionally, as I previously described, the right to protect intellectual property is balanced against the right to conduct a business. Once the balance shifts significantly to one side of the scale, the resolution is clear: the measure is of such a great benefit that it simply must be accommodated by the ISP. Consequently, the implementation of digital

---

[59] *See id.* ¶ 48.

[60] 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.

[60] *See id.* ¶47.

[61] *See Newzbin2*, *supra* note 35, at 162.

[62] The Court emphasized 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*, *supra* note 42, at ¶ 36 (citing L'Oreal SA & Ors, [2010] EWCA (Civ) 535 at ¶ 139).

[63] 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*, *supra* note 42, at ¶ 37.

[64] *See SABAM*, *supra* note 42, at ¶ 47.

[65] *See id.* ¶ 48.

[66] *Id*.

[67] *Id*. 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).

[68] *See SABAM*, *supra* note 42, at ¶ 48.

[69] *Newzbin2*, *supra* note 35, at 177.

fingerprinting technology may be something that a national court could order, provided it does not run afoul of the restriction on general monitoring.

¶21 Even without a court injunction, it may be in the best interest of the ISP, intermediary, or website host to install a digital fingerprint system. In the high stakes world of content delivery, it is in the best interest of service providers to foster close ties with big content creators in order to secure lucrative distribution contracts. Imagine the backlash from the content provider industry if a website gains a reputation as place to watch unauthorized streaming of videos, events or sports. Website hosts that allow widespread online piracy will quickly find themselves on the outside of the legal streaming industry. In addition, lawsuits involving large industry players, such as record labels or movie distributors, are expensive, time-consuming, distracting, and occurring with greater regularity. These considerations, coupled with aggressive government actions such as seizure of domain names for the broadcasting of "live" videos of sporting events and television programing, are beginning to create an online world that insists upon ISPs policing activities.[70]

¶22 Fortunately, the *SABAM* court did not completely overlook the individual as an important stakeholder in the online world. The court highlights:

> [The blocking] injunction could potentially undermine freedom of information since that system might not distinguish adequately between unlawful content and lawful content, with the result that its introduction could lead to the blocking of lawful communications.[71]

In the situation of potential over-capture, the court states that the blocking of lawful activity might undermine the freedom of information protections enshrined in the Charter of Fundamental Rights of the European Union.[72] Within the E.U. Charter, individuals are provided freedom of information[73] which, according to international law, can only be restricted in certain circumstances: "to protect the rights and reputations of others or to protect national security, public order, public health or morals."[74] While this language seems remarkably broad, the majority of commentators insist that these restrictions are to occur only in the narrowest of circumstances where there is a real risk of harm to a legitimate interest. This language is broadly explained to require that any restrictions be

---

[70] There are already moves in the E.U. to require ISPs to police the interest for terrorist activities. Called CleanIT, the proposal has far reaching impacts for ISP online policing of the Internet for 'criminal' and hence allowed policing activity. *See* Jillian C. York and Katitza Rodriguez, *Cleansing the Internet of Terrorism: Leaked EU Proposal Would Erode Civil Liberties*, ELECTRONIC FRONTIER FOUNDATION (Sept. 26, 2012), https://www.eff.org/deeplinks/2012/09/cleansing-internet-terrorism-leaked-eu-proposal-would-erode-civil-liberties (discussing the CleanIT system and its potential over-reaching impacts).

[71] *See SABAM*, *supra* note 42; *see also* Press Release No 126/2011, Court of Justice of the European Union, (Nov. 2011), *available at* http://curia.europa.eu/jcms/upload/docs/application/pdf/2011-11/cp110126en.pdf (discussing the EU law precludes the imposition of an injunction by a national court which requires an Internet service provider to install a filtering system with a view to preventing the illegal downloading of files); Press Release No 11/12, Court of Justice of the European Union (Feb. 16, 2012), *available at* http://curia.europa.eu/jcms/upload/docs/application/pdf/2012-02/cp120011en.pdf (explaining that the owner of an online social network cannot be obliged to install a general filtering system, covering all its users, in order to prevent the unlawful use of musical and audio-visual work).

[72] *See* Charter, *supra* note 51.

[73] *See id.* art. 11.

[74] International Covenant on Civil and Political Rights art. 19 § 3, Dec. 19, 1966 U.N.T.S. 14668.

limited to situations where there is a significant risk of serious and imminent harm with close causal link between the risk of harm and the expression.[75] While the expression does not seem to implicate general expression or posting of communication online, one must appreciate that such communication should be considered to fall within the provisions. Moreover, the provisions are especially relevant in relation to the criticism and debate concerning public issues, such as those previously highlighted with the Democratic National Convention or political rallies/uprisings. In these situations, commentators agree that the law must not be misused to censor criticism and debate of public issues.[76]

¶23 In addition to the Charter, the EU Personal Data Directive[77] and the EU Electronic Privacy and Communications Directive[78] add to the framework for protecting EU citizens' privacy and personal data. Most relevant to the issue at hand are those rights within the Communications Directive. Briefly, Member States are prohibited from listening to, taping, storing, intercepting, or otherwise conducting surveillance of communications[79] and related traffic data unless the users have given their consent.[80] The Directive also contemplates an exception to the monitoring and gathering of information in the situations where the adopted legislative measures "constitute[s] a necessary, appropriate and proportionate measure for the prevention, investigation, detection and prosecution of criminal offences."[81] Currently, there is no provision defining intellectual property right infringements as a criminal offense.[82] However, there are several treaties and other legal measures currently in discussions that may create a criminal offense in these instances. Should one of these legislative texts be adopted, the Communications Directive specifies that Member States may "adopt legislative measures providing for the retention of data for a limited period,"[83] on the condition that the retention is done in the pursuit of criminal offenses.[84] While the application of this Directive to the broadcasting

---

[75] *See* UNITED NATIONS, Human Rights Committee, General Comment 34, ¶¶ 23–33 (Sept. 12, 2011), http://www2.ohchr.org/english/bodies/hrc/comments.htm.

[76] *See id*. ¶ 38.

[77] *Directive on The Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data*, 1995 O.J. (L281) 31.

[78] *Directive Concerning The Processing Of Personal Data And The Protection Of Privacy In The Electronic Communications Sector*, 2002 O.J. (L201) 37, *as amended* by 2006 O.J. (L105) 54 and 2009 O.J. (L337) 11 [hereinafter 'Communications Directive'].

[79] *See id.* art. 2 § d. "Communication" means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information." *Id*.

[80] *See id.* art. 5 §1.

[81] *Id.* art. 15 § 1.

[82] This was one of the main issues in the failure of the Anti-Counterfeiting Trade Agreement (ACTA). 24 June 2011, COM(2011)0380, http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0380:FIN:EN:PDF (visited 14 April 2013). Of course, this is not the case in the US. *See* 18 U.S.C. § 2319 (2006) (criminal infringement of a copyright). Nor is it necessarily true when the infringement activity is substantial. *See* Agreement on Trade-Related Aspects of Intellectual Property Rights art. 61, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299 (requiring signatory countries to establish criminal procedures and penalties in cases of "willful trademark counterfeiting or copyright piracy on a commercial scale").

[83] Communications Directive, *supra* note 78, art. 15 § 1.

[84] *Id.*

of video is somewhat doubtful, the provisions may apply to certain types of communications that involve online piracy. In the case that this Directive were to apply to the particular medium of communication in question, it seems reasonably clear that interception of communications could occur if the party consents or if a criminal offense was present in the particular circumstances. Keep in mind, as previously discussed in Part I, a large portion of the Internet activity occurs on or within private sites governed by terms of agreement. In such cases, it is easy to imagine that consent to monitor and intercept communications will be present within these agreements.

¶24 Of course, the recent *SABAM* case suggests that these questions must be considered in light of the prescribed balance considerations. There is no specific language within the discussed texts that suggests that blocking (and storing), for the purposes of assessment of the lawfulness of the activity, cannot occur subject to some restrictions. For example, if the blocking was limited in duration, done for the purpose of assessment of the lawfulness of the communication, and completed in a timely manner that allows for the immediate return of the lawful communication, it might not run afoul of the law. In fact, it may comport to the balance between the intellectual property right holders and the individuals' right to communication, which has become a hallmark of the *SABAM* case. In the situation that a service provider undertook a limited burden or no burden in the determination of lawfulness of the communication, the triad would be complete and no party would be able to argue against the implementation of a digital fingerprinting system. Of course, this assumes that digital fingerprinting technology can be completed relatively quickly, has a means to store the communication while it is assessed, has a mechanism to challenge decisions of unlawfulness, and has the ability to restore the communication once a determination of lawfulness is completed.

B. The United States and the DMCA

¶25 United States courts have faced ISP issues eerily similar to the *Newzbin2* and *SABAM* cases. In the case of *Religious Technology Center v. Netcom On-Line Communication Services*,[85] the Northern District of California found that once the copyright holder had put the ISP on notice of the infringing content, the act of providing the distribution of the infringement could amount to substantial participation. In language remarkably similar to *Newsbin2* and *SABAM* court language, the California court noted:

> Providing a service that allows for the automatic distribution of all Usenet postings, infringing and noninfringing, goes well beyond renting a premises to an infringer. . . . Thus, it is fair, assuming Netcom is able to take simple measures to prevent further damage to plaintiffs' copyrighted works, to hold Netcom liable for contributory infringement where Netcom has knowledge of [the direct infringer's] infringing postings yet continues to aid in the accomplishment of [the infringer's] purpose of publicly distributing the postings.[86]

[85] Religious Tech. Ctr. v. Netcom Online Communic'n Serv., 907 F. Supp. 1361 (N.D. Cal. 1995).
[86] *Id.* at 1375.

¶26 In 1995 there were arguments for the standard being: (1) technology that allowed distribution and not mere rental of space online, (2) knowledge of infringing activity, and (3) the availability of simple measure to prevent the piracy.[87] The outcome of this case sent shockwaves through ISPs as it seemingly imposed a burden to police the activity of its users in order to prevent online piracy. Failing to undertake simple measures to prevent online piracy meant that ISPs would be liable for copyright infringement.

¶27 In direct response to this potentially broad liability, Congress enacted the Digital Millennium Copyright Act[88] and specifically included a section to protect ISPs from liability provided that the ISP takes expeditious action to remove allegedly infringing content.[89] Similar to the E.U. law, under the DMCA, an ISP can be issued "injunctions on such terms as it [the court] may deem reasonable to prevent or restrain infringement of a copyright."[90] These court injunctions can be directed in two ways: (1) "restraining the service provider from providing access to infringing material or activity residing at a particular online site on the provider's system or network,"[91] and (2) "restraining the service provider from providing access to a subscriber or account holder of the service provider's system or network who is engaging in infringing activity and is identified in the order, by terminating the accounts of the subscriber or account holder that are specified in the order."[92] However, in language that does not track current EU law, the DMCA limits relief to "the *least burdensome* to the service provider among the forms of relief comparably effective for that purpose."[93] This phrase makes clear that the court is not asked to perform any type of balance between the various stakeholders. Instead, under the DMCA the service provider may be ordered to undertake the least burdensome action that would be "comparably effective" in ending the infringing activities of the user or website activity. This provision does not consider the *total* burden on the ISP; instead, it prescribes that the selected form of relief be the least burdensome of the relief available. The least burdensome standard is a significant departure from the E.U. standard, and it fails to address the issue of the overall burden on the ISP.

¶28 Moreover, the DMCA specifically prescribes that the burden of investigation is not to be placed on the ISP.[94] As a result, while the standard is one of least burdensome relief

---

[87] *Id*.

[88] 17 U.S.C. § 512 (2006). In describing the "dual purpose and balance" of the DMCA, the court in *Verizon Internet Services* highlighted:

> Congress . . . created tradeoffs within the DMCA: service providers would receive liability protections in exchange for assisting copyright owners in identifying and dealing with infringers who misuse the service providers' systems. At the same time, copyright owners would forgo pursuing service providers for the copyright infringement of their users, in exchange for assistance in identifying and acting against those infringers.

In re Verizon Internet Servs., Inc., 240 F. Supp.2d 24, 37 (D.D.C.), *rev'd sub nom*. Recording Indus. Ass'n of Am. v. Verizon Internet Servs., 351 F.3d 1229 (D.C. Cir. 2003).

[89] For an introduction to the background of the drafting of the DMCA, see Jon M. Garon, *Tidying Up the Internet: Take Down of Unauthorized Content under Copyright, Trademark and Defamation Law*, N. KY. U. CHASE L. & INFO. INST., Working Paper Series, (March 2012) *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2029326.

[90] 17 U.S.C. § 502(a) (2006).

[91] *Id*. at § 512(j)(1)(A)(i).

[92] *Id*. at § 512(j)(1)(A)(ii).

[93] *Id*. at § 512(j)(i)(3) (emphasis added).

[94] Capitol Records, Inc. v. MP3tunes, LLC, 821 F. Supp. 2d 627 (S.D.N.Y. 2011) (citing 17 U.S.C. § 512(m) (2006)). In fact, the court in *Aimster* noted that this provision of § 512 "represents a legislative

of the available relief, no ISP may be ordered to investigate activity in an effort to prevent online piracy. Accordingly, under the DMCA, a service provider with actual knowledge or awareness of infringing activity[95] can be ordered by the court to: (1) block or remove an individual as a customer; (2) block or remove a specific file(s); and/or (3) block or shut down a specific website.[96] However, unlike E.U. law, a service provider cannot be ordered to monitor activity, regardless of the level of specificity of the request.[97] And any order issued does not need to be done in light of a balance Instead, the standard is one of the "least burdensome action" that would be "comparably effective" in ending the infringing activities of the user(s) or website activity.

¶29 In a significant departure from current E.U. law, the DMCA protects an ISP from claims arising from the removal or denial of access to content. In this instance, the language of the DMCA is important to the debate:

> A service provider shall not be liable to any person for any claim based on the service provider's good faith disabling of access to, or removal of, material or activity claimed to be infringing or based on facts or circumstances from which infringing activity is apparent, regardless of whether the material or activity is ultimately determined to be infringing.[98]

¶30 Under the DMCA, the decisive factor is "good faith," which is a notoriously slippery term in all areas of law. But the real issue here is the absolute protection that arises for ISPs acting in "good faith." An ISP is protected when it removes material or disables access to a website—regardless of the ultimate determination of the lawfulness of the material. In the cooperation focused online world that now contains the marriage between service providers and intellectual property right holders, this provision may just spell doom for individual stakeholders as their interests will rarely impact practical, business-based decisions, especially with the extreme limited liability protections that exist for ISPs.

---

determination that copyright owners must themselves bear the burden of policing for infringing activity — service providers are under no such duty." *In re* Aimster Copyright Litig., 252 F.Supp.2d 634, 657 (N.D. Ill. 2002), *aff'd*, 334 F.3d 643 (7th Cir. 2003).

[95] DMCA recognizes two standards, actual knowledge or awareness, described as "circumstances from which infringing activity is apparent." 17 U.S.C. § 512(c)(1)(A)(i) and (ii) (2006).

[96] 17 U.S.C. § 502(a) (2006). Of course, the ability of a court injunction shutting down a website under a DMCA provision is an ongoing issue as the Wikileaks case emphasizes. *See* Bank Julius Baer & Co. v. Wikileaks, 535 F.Supp.2d 980 (N.D. Cal. 2008). The entire case history, including amicus briefs, can be found at http://dockets.justia.com/docket/california/candce/3:2008cv00824/200125/.

[97] Some argue there is one exception to my assertion, 'repeat infringers.' As noted by the court in *Aimster*:

> The [DMCA] provides a series of safe harbors for Internet service providers and related entities, but none in which Aimster can moor. . . . The common element of [the DMCA]'s safe harbors is that the service provider must do what it can reasonably be asked to do to prevent the use of its service by "repeat infringers."

Aimster, 334 F.3d at 655.

[98] 17 U.S.C. § 512(g)(1) (2006) (emphasis added). Of course, there are exceptions to this protection, such as that the ISP has to provide notice and allow for challenges to the good faith removal. Moreover, the DMCA also provides that the material must be kept and has to have the ability to be restored. 17 U.S.C. § 512(g)(2)(C) (2006).

¶31 Without a doubt when this provision was written it was groundbreaking and essential for the further development of the Internet.[99] It protected ISPs from a new and unpredictable digital landscape that included a growing concern for online piracy. At the time, no one could predict how online users would behave and no one wanted to envision ISPs being legally responsible for ”facilitating” copyright infringement,[100] especially when no one really knew if the vast majority of Internet users would engage in non-infringing uses of the Internet.[101] The protection was essential for ISPs. But such protection is now creating issues for ISPs as the speed of communication[102] coupled with serious advances in hardware and software development have substantially changed the online world. These substantial changes in the online environment have demanded that ISPs react with significantly less time to evaluate claims prompting an increased use of technology to assist in the assessment function.

¶32 While the DMCA provides absolute protection in terms of ISP liability, it limits the protections by prescribing procedures that ISPs must take in response to a notice of infringing activity. Focus should now be placed on the phrase ‘activity *claimed* to be infringing’ as this is the turning point in terms of digital fingerprinting. Within the practical realities of the system, an intellectual property right holder is able to serve notice of infringing activity upon a service provider and the service provider disables access and/or removes the material.[103] Within the context of current technology, digital fingerprinting allows studios and individuals to ”claim” a significant amount of material as infringing. The ability to claim material as infringing is an unfettered one. Consequently, the material may be removed even if the material is not within the intellectual property portfolio of the entity making the claim, and the ISPs are protected from liability provided the take-down action is done in good faith.

¶33 In some ways it is even more concerning that the law promotes incentives for the ISP to take the assertion at face value. As a result, any claim of infringing activity results in the material being removed at least temporarily. In terms of wrongfully identified material, the only mechanism in place to challenge the claim of infringing activity is to file a challenge, known as a counter-notification,”[104] with the entity that removed or disabled access (the service provider). Under the DMCA, the entity filing the take-down notice must then notify the ISP within ten business days that they have filed an action seeking a court order to restrain the infringing activity.[105] Without a notice of a legal

---

[99] The Act’s legislative history indicates that Congress wanted to provide service providers with “more certainty . . . in order to attract the substantial investments necessary to continue the expansion and upgrading of the Internet.” 144 CONG. REC. S11, 889 (daily ed. Oct. 2, 1998) (statement of Sen. Hatch).

[100] *See* Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417 (1984).

[101] *See* MGM Studios, Inc. v. Grokster, Ltd., 545 U.S. 913 (2005).

[102] Keep in mind that in the U.S. the Communications Decency Act (CDA 230) relieves sites of liability for their users' content. In other words, under CDA 230, only users have legal responsibility over what they post. However, CDA 230 does not apply to intellectual property claims and federal criminal law. Telecommunications Act of 1996 (CDA), 47 U.S.C. § 230, P.L. No. 104-104, 110 Stat. 56 (1996). For a further discussion of CDA 230 and its possible protections, see Bart Szewczyk, Patrick Carome, & Colin Rushing, *Online Intermediaries and Third Party Content under EU and US Laws*, 83 MEDIA LAW RESOURCE CENTER BULLETIN 3, 83–94 (2007) (arguing that Section 230 may be available in the US as a defense to a foreign judgment that is inconsistent with Section 230’s protections).

[103] *See* 17 U.S.C. § 512(g)(2) (2006).

[104] *See id.* § 512(g)(3).

[105] *See id.* § 512(g)(2)(c).

action, the service provider must restore the material within fourteen days.[106] Of course, this results in the material not being available for a significant period, which is concerning when the material in question is part of a stream or a timely debate topic. Recall the Hugo awards or the Democratic National Convention.[107] These were both streamed "next-to-live"; no one wanted to watch a tape-delayed broadcast. Shutting down this stream ended the "next-to-live" broadcast. Restoring the material at a significantly later time is simply not the same to the online community or to the advertisers and others drawing a benefit from an engaged first-to-know-the-information audience. This particular mechanism has a serious potential for abuse and may in fact be de facto censorship.

¶34 It is equally concerning that the policies surrounding the use of digital fingerprinting technology allow entities to upload and tag information even if the material is not within their intellectual property portfolio. In these situations, the only real means to prevent continual flagging of the material is for the rightful holder of the material to challenge the "asserted" ownership of the entity uploading the material into the digital database. At this time, most of the digital fingerprinting technology systems do not anticipate the need for this protection and many have no mechanism in place to rectify this issue. Consequently, one can appreciate several crucial issues: (1) mere notice of infringing activity causes the material to be removed or blocked; (2) for the material to be restored, the individual must file a counter-notification claim and then may need to succeed in proving ownership or appropriate licensing rights in court; (3) the ISP is protected from liability based mainly on the nebulous requirement that it act in "good faith"; (4) the entity originally filing the notice suffers no real consequence for notices that are inaccurate, poorly researched, or flat-out wrong;[108] and (5) there is a lack of effective policy governing how oversight of the technology in question and challenges to holder rights.

IV. MINOR ADJUSTMENTS ARE NEEDED IN KEY PROBLEM AREAS

¶35 As can be gathered from the above comparison, existing legal texts and cases are demanding the recognition of a balance of interests between three primary stakeholders: (1) the service providers, (2) the right holders, and (3) the individual users. Within the United States, the right holder is protected via a simple notice system, the individual is protected with a right of appeal, and the ISP is protected from liability as long as it quickly responds to take-down requests. At the time of drafting, the approach advanced by the United States was balanced, basically fair, and provided full coverage. However, today the speed and ease of online communications and other technology advancements have created a different online world. Consequently, the old balances are no longer working within the United States: (1) the allegedly infringing material is offline for potentially fourteen days—even if it is legal; (2) ISPs are in the position of honoring the majority of take-down requests—presented to them in the millions; (3) right holders are ready and willing to pay for services that monitor the Internet for infringing material—all

[106] *See id.*

[107] *See* Newitz, *supra* note 7 and corresponding text; Singel, *supra* note 7 and corresponding text.

[108] The notification is submitted under penalty of perjury for inaccurate information, a remedy rarely used. *See* 17 U.S.C. § 512(c)(3)(vi) (2006).

while monetization allows infringing material to play so long as you pay; and (4) the law allows the use of terms of service to force users to consent to the use of digital fingerprinting technology, despite serious issues concerning both the technology and the policies that surround its use.

¶36 In the European Union, the *SABAM* case has prompted a significantly different balance, one that includes the concept of fundamental rights of the stakeholders. Despite a different starting point, the need for a balanced approach to preventing online piracy has resulted in essentially the same practical outcome. ISPs are burdened with a need to cooperate in preventing copyright infringement, and as such, they too have turned to digital fingerprint technology in an effort to avoid liability for not doing enough to prevent online piracy. While the reason for the use of digital fingerprinting technology arises from a different conceptual burden, both the European Union and the United States are facing the same set of practical issues in relation to the use of technology. Digital fingerprinting is being used as a "fix" to all that ails. The technology is allowed as the ISPs have no reason to prevent the use of such a system, and the law fails to prevent its misuse and/or or the ISPs must protect themselves from liability for doing too little to prevent online piracy. In both instances, digital technology seems to be the adopted cure-all. Accordingly, the law must be altered to regulate the use of this technology as the system and the policies surrounding its use are not protecting the rights of online users. Consequently, the balance between the online stakeholders has been lost. The question then becomes: what adjustments can be made to rectify the imbalance?

A. EU Cooperative Burdens Are Based on a Narrow Focus of the ISPs' Burdens

¶37 In contrast to the DMCA, the *Sabam* case clearly establishes that ISPs have a fundamental right to operate their business without an undue burden.[109] 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 ISPs should include considerations of the high volume of activity being requested by intellectual property right holders to protect their intellectual property rights. For example, Verizon notes that it is often sent automated "take-down" notices by the thousands.[110] Meanwhile, Google reports it has received 6,312,528 uniform resource locators (URLs) removal requests within the past month.[111] Given the sheer volume of these requests it is worth asking: in examining the proper degree of burden being placed on a business, shouldn't a comprehensive examination of the entire burden be the standard? Certainly the burden on the business is only truly measured when considered in light of *all* of the actions requested by *all* intellectual property right holders.

¶38 Google is the perfect example to consider in this debate. Google is one of the noted ISPs that takes a semi-hands-on approach to the online world by complying with some,

---

[109] *See* SABAM, *supra* note 42. *See supra* notes 36-47 and corresponding text.

[110] *See* Deutsch, *supra* note 22 and corresponding text.

[111] *See Google Transparency Report*, GOOGLE (Sept. 24, 2012), *available at* http://www.google.com/transparencyreport/removals/copyright/. This number is not outrageously high. *See Google Receives 1.5m Takedown Requests a Week*, TELEGRAPH ONLINE (Sept. 28, 2012) http://www.telegraph.co.uk/technology/google/9502877/Google-receives-1.5m-takedown-requests-a-week.html (discussing the number of take down requests).

but not all, take down requests.[112] To catch erroneous requests someone—or probably a very large team of "someones"—is tasked with considering each request individually. But this is troubling in the context of E.U. and U.S. laws, both of which place a high value on not burdening ISPs with the protection of intellectual property rights. Taken together, court orders and take down requests create an unfair burden for ISPs.[113] The need for ISPs to employ individuals or digital technology to police Internet activity is a disturbing trend and places too high of a burden on ISPs.[114] The creation of a cooperative burden of preventing online piracy and advancements in technology are causing ISPs to undertake much too great a role in the protection of intellectual property rights. The law and the courts must seek to rebalance the burdens emphasizing the intellectual property right holder's responsibility in terms of identification and enforcement costs. Within the U.S., this can only be accomplished if the law revisits the system of notice-and-take-down requests and considers the appropriate role and burden of ISPs in evaluating these requests. Within the E.U., the law must begin to envision the burden placed on the ISPs beyond a single request and resist the urge to adopt the U.S.-based notice and takedown system with adjustments being made for advancing technology. Finally, the difference between U.S. and E.U legislative approaches demonstrates the need to not only update the law, but to harmonize the approach to the protection of intellectual property rights and the burdens to be placed on Internet providers.

B. The Existing Legal Regime Breaks Down in Relation to Live Streaming

¶39 Online video content as a source of communications and commentary is a growing reality in the digital age. According to online research institution comScore, 188 million U.S. Internet users watched 37.7 billion online content videos in August 2012.[115] In fact, this is the highest number of Internet users reported to be watching online video content within a given month.[116] Yet, despite the significant rise in online video content delivery and the certain corresponding increase in live streaming, the law has failed to adequately adjust to advancement in these delivery methods.

¶40 The notice-and-take-down regime created by the DMCA allows copyright holders to send a notice to an online hosting service when they find their copyright being violated.[117] The online service then removes the content. However, there is nothing within the law that places a time limit on the response. Instead the timeframe is one of

[112] For example, senior copyright counsel at Google, Fred von Lohmann, reports that Google attempts to "catch erroneous or abusive removal requests" and in doing so does not honor all requests for removal. *See* Fred von Lohmann, *Transparency for copyright removals in search*, GOOGLEOFFICIALBLOG (May 24, 2012), http://googleblog.blogspot.com/2012/05/transparency-for-copyright-removals-in.html.

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

[114] The practical impact of this technology may just be creating a significant increase in take down requests, as highlighted by the Google transparency report which shows a trebling of take down requests from May to July. *See Google Transparency Report*, *supra* note 111. Keep in mind, this timeframe is also right after the decision in *SABAM* that created the 'cooperative burden' in the EU.

[115] *See comScore Releases August 2012 U.S. Online Video Rankings*, COMSCORE (Sept. 19, 2012), http://www.comscore.com/Press_Events/Press_Releases/2012/9/comScore_Releases_August_2012_U.S._Online_Video_Rankings.

[116] *Id.*

[117] *See* DMCA discussion, *supra* notes 85–88 and corresponding text.

"expeditious" removal.[118] Unsurprisingly, response times vary under this loose standard. For example, Google reports that it takes an average of 11 hours to respond to take-down requests.[119] But few live streaming events last longer than a few hours and few take place over eleven hours. As a result, live streaming almost always escapes the reach of a shut-down request. On the other hand, if a live stream event is taken down, the user who posted it has no immediate recourse to have the video restored. Instead, the user must file a counter-notice and wait for approximately 14 days.[120] The usefulness and marketability of the live stream is all but eliminated in these circumstances. Consequently, at a minimum the law needs to be updated to better accommodate advancements in broadcasting and communications technology.

C. A Party with Skin in the Game is Making All the Final Decisions

¶41 An ISP that must adjudicate between the removal of content that is allegedly illegal and exposure of its own liability will tend to remove the content that has been flagged for removal.[121] However, this is not always the case. As previously discussed, Google has a team in place to review take-down requests and decide which should be honored. The online community is fortunate to have ISPs willing to take up the mantle of balancing the interests of intellectual property right holders and individual users, especially since the undertaking causes them to incur a great amount of cost and potential liability. However, no regime as important as this should rely upon the good faith of a business, especially when the business making the determinations has such a large stake in the determinations. In contrast, not every service provider is able, or willing, to take on a task associated with such a high cost and potentially significant liability.

¶42 More concerning is the absence of regulation, guidance, or other information that assists ISPs in making these determinations and/or guidance that places restrictions upon the factors that can be used to make such determinations. While most commentators highlight Google's informal corporate motto "Don't Be Evil"[122] as reflective of intent to balance stakeholder interests in the online world, one can appreciate that not all entities making decisions subscribe to this corporate philosophy. And even when service providers subscribe to Google's philosophy, these determinations are often subjective and are thus open to great debate in terms of meaning and practical application.[123] Without a

---

[118] *See id.*

[119] *See* von Lohmann, *supra* note 112.

[120] *See* DMCA discussion, *supra* notes 104–07 and corresponding text.

[121] Researchers in Great Britain demonstrated that providers in the UK removed content that was perfectly compliant with copyright law in greater numbers than their counterparts in the Netherlands. *See* C. Ahlert, C. Marsden & C. Yung, *How 'Liberty' Disappeared from Cyberspace: The Mystery Shopper Tests Internet Content Self-Regulation* (2004), *available at* http://pcmlp.socleg.ox.ac.uk/sites/pcmlp.socleg.ox.ac.uk/files/liberty.pdf (last visited Aug. 15, 2012). *See also* S. Katyal, *The New Surveillance*, CASE W. RES. L. REV. 54, 367-68 (2003); S. Kreimer, *Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link*, U. PA. L. REV. 155, 32–33 (2006); Alfred C. Yen, *Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and the First Amendment*, GEO. L. J. 88, 188889 (2000); W. Seltzer, *Intermediaries, Incentive Misalignments, and the Shape of Online Speech?* (Berkman Ctr. for Internet and Soc'y, Harvard Law School, Working Paper 2009).

[122] *See* Philipp Lenssen, *Paul Buchheit on Gmail, AdSense and More*, GOOGLE BLOGOSCOPED (Jan. 25, 2001), http://blogoscoped.com/archive/2007-07-16-n55.html.

[123] Even Google cannot escape some overzealous copyright-based shut-downs. *See* Mike Masnick,

level of guidance and/or regulation service providers are left to their own devices to make these determinations. It is not hard to imagine that they might be based on hidden agendas, secret algorithms, and future business desires. While there is nothing inherently wrong with this self-regulatory approach, some level of guidance is certainly needed to protect individual's fundamental rights. Consequently, there is a desperate need for a level of guidance on the design and implementation of the response to take-down requests that insists upon considerations being given to the protection of all stakeholders.

D. The Current System Over-Captures/Identifies Online Material Without Providing Appropriate Protections

¶43 As discussed extensively above, the problem of over-capture/identification of information is a growing problem as technology is being used as a mainstream effort to fight online piracy. This problem is exacerbated since the law does not provide for protection of an individual's information/communications. Although the US does provide protections when an individual's information/communication is removed from a website,[124] no law in the E.U. or U.S. provides protections when an *entire* website is blocked. As argued by the attorneys for Kyle Goodwin in the Megaupload case, *United States vs. Kim Dotcom*:[125]

> 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.[126]

Google's Copyright Crackdown Punishes Author For Torrenting His Own Book, TECHDIRT (Sept. 27, 2012) (describing the plight of an author who linked to his own book that was made available on PirateBay).

[124] 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* Lee Edward, *Decoding the DMCA Safe Harbors*, 32 COLUM. J. L. & THE ARTS 233 (2009); Lydia P. Loren, *Deterring Abuse of the Copyright Takedown Regime by Taking Misrepresentation Claims Seriously* 46 WAKE FOREST L. REV. 745 (2011); Ira Nathenson, *Looking for Fair Use in the DMCA's Safety Dance*, 3 AKRON INTEL. PROP. J. 1, 121-170 (2009). In contrast, "the E-Commerce Directive lacks a notice and take-down procedure like the one set forth in section 512(c)(3) of the DMCA." Peguera, Miquel, *The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems*, 32 COLUM. J. L. & ARTS 481 (2009). There are widespread complaints about this process. 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) (arguing for reforms to protect online speech); Enrico Bonadio, *File Sharing, Copyright and Freedom of Expression*, 33 EUROPEAN INTELL. PROP REV. 10 (2011) (discussing the limits to freedom of expression in Europe compared to the US).

[125] Indictment, U.S. v. Dotcom et al., No. 1:12CR3 (E.D. Va. Jan. 5, 2012), *available at* http://www.citmedialaw.org/sites/citmedialaw.org/files/2012-01-05-Indictment.pdf. *See also* Nathan Olivarez-Giles, *Justice Department indictment of MegaUpload*, LA TIMES (Jan. 19, 2012), http://documents.latimes.com/justice-department-indictment-file-sharing-site-megaupload/ (discussing the Megaupload case).

[126] Brief Of Interested Party Kyle Goodwin In Support Of Emergency Motion For Protective Order By Non-Party Carpathia Hosting, Inc. And For Additional Relief at 1 U.S. v. Kim Dotcom, No. 1:12CR3 (E.D. Va. Mar. 30, 2012) 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 (Apr. 13, 2012), http://news.cnet.com/8301-1023_3-57413506-93/u.s-tries-to-silence-megaupload-lawyers-on-issue-of-user-data/ (discussing the case and the protection of user data); David Kravets, *Judge Won't Purge Megaupload User Data, At Least Not Yet*, WIRED (Apr. 13, 2012),

¶44 The absence of protections in terms of the information that is lawfully stored on a website is a troubling gap in the current legal regime. In the absence of legal proscriptions, the harmed party needs to seek the assistance of the court to craft the necessary protections. At a minimum, one would expect that the court would require: (1) that a filtering or similar system would be set up to return to the rightful owner any information/contents or communications that are clearly not the subject of an intellectual property right holder claim against the website/user; (2) the ability of the individual that stored or transmitted the information to demonstrate the contents are of a lawful use/activity; and (3) the safekeeping of the information until any issues are resolved. But again, these protections would need to be delineated by the court and are not prescribed as a matter of law. This leaves individual users at a significant disadvantage when a website is shut down as their information is no longer available and there is often no time frame for the restoration of the website or the return of the material. Moreover, any actions in relation to the material would result in costs to the storage providers, in terms of both storage and filtering of lawful material. Thus, laws need to be designed to ensure that information is protected, that retrieval of lawful information is possible, and that the costs associated with these actions are appropriately considered within the overall balance.

E. The System is Automated with No Common Sense Button

¶45 As discussed above, numerous digital fingerprinting technology providers use a system that is fully automated. But while technology can make many determinations, there are always legal grey areas within overlapping and divergent legal regimes that demand a level of context-based judgments. Recall the Hugo Awards and the NASA Mars landing video,[127] both of which should have been allowed to continue to be live streamed, yet were shut down. As the technology currently functions, it: (1) over captures information and communications; (2) is biased in favor of mere assertions of intellectual property rights holders; (3) has no oversight concerning data entry; and (4) uses little to no human intervention or context based determinations in the take-down process. Possibly most concerning is the use of a system that automatically removes information without the ability for a level of human intervention, decision making, and discretion in light of the circumstance. In instances such as the Hugo Awards, the system must have a "common sense button"[128] that allows the video, audio file, or stream to continue to be available, despite an automated shut down response. Moreover, the entity or entities making the shut-down determinations must be protected under the law. These protections must exist regardless of their determination of the lawful or unlawful nature of the material, provided the decision is made in good faith with a level of human intervention. This protection would shield ISPs from liability, from right holders and

http://www.wired.com/threatlevel/2012/04/megaupload-data-flap/ (discussing the delay in the decision in relation to the release of data). As of Sept. 27, the New Zealand Prime Minster has apologized to Kim Dotcom, and the MegaUpload site may relaunch soon. *See* Matt Burns, *New Zealand Prime Minister Apologizes To Kim Dotcom As Megaupload Nears Relaunch*, TECHCRUNCH (Sept. 27, 2012), http://techcrunch.com/2012/09/27/new-zealand-prime-minister-apologizes-to-kim-dotcom-as-megaupload-nears-relaunch/ (discussing New Zealand perceived failure to support Dotcom against the legal claims).

[127] *See* Newitz, *supra* note 7 and corresponding text; Singel, *supra* note 7 and corresponding text.

[128] *See* Higgins, *supra* note 7 and corresponding text.

individuals,[129] and allow for the return of a balance between the two often conflicting stakeholder interests.

F. The System is Easily Abused

¶46 A common and ongoing problem with the existing digital fingerprinting technology occurs in the policy that allows for ”alleged” intellectual property right holders to upload material and tag it within the system without verification or authentication of legally recognized intellectual property rights. Unfortunately, the tendency of some right holders to over claim information is not one that is unique to the digital fingerprinting technology and as such, it is not really surprising that protections must be put in place to prevent attempts to over claim rights. For example, in the cases of *CPI v Robinson*,[130] *Twentieth Century Fox v Newzbin*,[131] and *Twentieth Century Fox v British Telecoms*[132] the plaintiffs encountered great difficulty in proving intellectual property rights that were essential to the furtherance of the proceedings. In each of these cases, the court refused to grant a wide injunction covering material that was not clearly within the ownership or exclusive license of the party seeking the injunction. But of course, these cases arose within the court system, and as such, a level of oversight prevented the abusive practice of over claiming. It is therefore concerning that no oversight is included within digital fingerprinting technology systems and that no jurisdiction places a legal requirement upon the system to prevent this type of abuse. In fact, the majority of systems fail to allow the rightful owner or exclusive license holder to contest wrongful claims of ownership. As such, the system is ripe for abuse and does not provide the necessary protections that right holders are entitled to expect.

¶47 Moreover, the law fails to penalize those that make wrongful or erroneous claims of intellectual property rights and/or those that file wrongful or erroneous take-down requests. The law places too high of reliance upon the honest nature of those entities that file take-down requests, a status that they no longer deserve. The advancement of technology and the ability to file simple online forms has created a notice-and-takedown system that rewards entities that over-file claims. The entities make these claims with full knowledge that the system is either automated and thus will implement requests without oversight or that they are human decision based systems overloaded with requests. This results in a serious abuse of the system by a single stakeholder. Instead, the system should require a level of oversight and should penalize those entities that abuse the system.

---

[129] Unfortunately, this would not protect ISP or the individuals that run them from the actions of a government official. Consider the issue in light of the Brazilian arrest of the head of Google’s operations in Brazil for failure to remove YouTube videos that attacked a mayoral candidate. *See* Jeff Fick & Amir Efrati, *Brazil to Arrest Google’s Local Chief*, WALL ST. J. (Sept. 25, 2012), http://online.wsj.com/article/SB10000872396390444813104578018673571930046.html (describing the initial order in response to the websites refusal to honor a court order requiring the removal of video); Adi Kamdar, *Shooting the Messenger: The Misfortunes of Google Brazil and the Need for Intermediary Protections*, ELECTRONIC FRONTIER FOUNDATION (Sept. 26, 2012), https://www.eff.org/deeplinks/2012/09/shooting-messenger-brazil (describing the full order, which also included a 24-hour shut down of Google and YouTube).

[130] [1986] 3 All E.R. 338, 364-5 (Eng.).

[131] [2010] EWHC 608 (Ch) (Eng.).

[132] [2011] EWHC 1981 (Ch) (Eng.).

G. The Online User is Often Forgotten and Without Legal Protections

¶48 When considering the need for protections and new legislative initiatives, one online stakeholder's interest that has been historically forgotten and must begin to draw the attention of the drafters: the individual users. Individual users need to be concerned that they are forgotten, as the law currently creates odd burdens and strange incentives that continue to ostracize these stakeholders. Without appropriate legal protections, Internet users will face a growing battle as the legal incentives[133] that encourage ISPs to create these systems which will continue to over identify and capture information. The reason behind this is simple. The online world where we post, publish, store, and communicate is provided by private entities. In most cases, these private entities can and do regulate our online behavior via the use of a detailed user/terms of service agreements, with few restrictions. These terms of service agreements regulate everything from what can be posted, to the service provider's response to the posting of inappropriate or infringing material. There is really nothing to prevent ISPs, intermediaries, and website hosts from implementing terms of service that include the use of digital fingerprinting technology to identify material. It will simply be a condition of storing and posting material, and generally using the Internet. However, as discussed above, the technology is fraught with issues, and the policies surrounding the use of the technology are often significantly one-sided in favor of the purported holder of the intellectual property right. As individual users we need to be concerned, the newly created cooperative burden placed on service providers and intermediaries has shifted the balance in the online world into an odd marriage between service providers and intellectual property right holders.[134] And this shift can and will be supported via the terms of service agreements widely imposed upon the online community. The law and the legal protections enshrined within it envisioned a much different balance within the online community.[135] Fortunately, individual users as important stakeholders are beginning to garner attention as demonstrated by the European Court of Justice's case of *SABAM v Scarlet Extended.*[136] None of these laws go far enough to protect individuals, however, as the incentives for ISPs to assist in policing the Internet for online piracy are simply too great at this time.

V. CONCLUSION

¶49 The United States and the European Union have long recognized the need to protect ISPs from potential liability arising from customers using their services to infringe intellectual property rights. The full parameters of these protections is being revisited by the courts as it has recently become clear that ISPs are in the best position to cooperate in the prevention of online piracy. The expectation of cooperation between intellectual property right holders and ISPs is creating an odd marriage of interests that frequently excludes considerations of the online rights of individuals. Moreover, the law has not yet accommodated the expectation of cooperation, and as such, ISPs will be subject to lawsuits from intellectual property right holders for not responding to take-

[133] *See* Raymond, *supra* note 36.
[134] *Id*.
[135] *Id*.
[136] *SABAM*, *supra* note 33.

down/shut-down requests. Furthermore, ISPs will be pursued by individuals for a failure to protect their information from reactionary measures demanded by right holders. This is an untenable situation that the law was specifically designed to prevent. Yet, the creation of a cooperative burden places service providers in a ”try it out and wait and see” situation, hoping for the best but fearing the worst in terms of liability. The response is predictable; return some of the burden to intellectual property right holders by allowing them to use technology to identify infringing activity online. However, the technology is not yet ready for wide scale use and is often accompanied by policy that allows over claiming of material in an effort to increase monetization. Again, a wrong set of incentives has created a poor response to online piracy. The law must react to these odd incentives arising from the creation of a cooperative policing burden being placed on the ISPs and must do so in a way that ensures all online stakeholders' rights are protected. The balance can only be restored by: (1) ensuring that ISPs are not burdened under the sheer weight of requests to protect intellectual property; (2) ensuring that ISPs are protected from liability arising from an ISP's unwillingness to honor a takedown request when the takedown request is clearly overreaching, or suffers from similar defect; (3) ensuring that the use of technology is employed with a level of oversight; (4) ensuring that any technology employed recognizes and provides appropriate avenues to contest wrongful claims of ownership and/or licensing rights; (5) ensuring that penalties exist and are enforced for the wrongful filing of take-down requests, or similar actions; and, (6) ensuring that the law is designed with an eye toward an ever growing use of streaming and other high speed communication and broadcasting technology.