TIME TO REBOOT?: DMCA 2.0

Donald P. Harris*

INTRODUCTION

Imagine this scenario. Mary Saint Francis was a longtime librarian of limited means. She had always dreamed of becoming a successful writer and living the way "the other half" lived, retiring from the library and traveling around the world. At 56, and after a number of unsuccessful and little known short stories, she was beginning to believe this would never happen. In March 2013, things changed. Mary wrote a saucy and stimulating novel about being a librarian: *The Real Life of a Librarian*. Surprisingly, *Real Life* became an instant success. Over the next year, Mary's novel achieved critical acclaim, was the subject of Oprah's Book of the Month, was the topic of numerous talk shows, and was discussed on various news and radio spots. Mary also traveled "the circuit," courtesy of her publisher, to promote the book. Mary's dream was soon to be realized—or so she thought.

Mary's novel also became the most downloaded book on the Internet. As a result, Mary did not get rich. In fact, Mary received very little proceeds from her novel due to unauthorized downloading. Dismayed, Mary questioned why people were able to upload, copy, and distribute her book without paying. Mary knew a little about copyright law and thought that having a copyright on her novel protected her, or that someone would (and should) be liable for unauthorized copying and infringement. Mary's publisher explained to her that under the 1998 Digital Millennium Copyright Act ("DMCA"), Internet Service Providers ("ISPs") were not liable for the copyright infringement of its subscribers as long as the ISPs followed certain guidelines. Mary could sue each of the individual infringers separately, but the cost of doing so would be prohibitive. Frustrated, Mary went back to work at the library, never to write again, and never to realize her dreams.

---

* Associate Professor, Temple Beasley School of Law. The author wishes to thank Edward Lee, Thomas Main, Salil Mehra, and David Post for their insightful comments. The author also thanks the participants of the 2014 Chicago Intellectual Property Series at Chicago Loyola University Law School, and the participants at the 2014 William S. Boyd School of Law, University of Nevada, Las Vegas Faculty Speaker Series for their suggestions, comments, and invitation to present earlier versions of this work. Finally, special thanks goes to Andrew Barron, Joseph Keller, Ana Pachner, Jessica Sganga, Paul Urbish, and Benjamin Walker for their excellent research assistance.

Individual authors are not the only ones who might complain about the current copyright scheme. While individual or small-scale copyright owners suffer relatively small scale infringement, large multimedia companies have argued that they stand to lose millions from massive copyright infringement. Infringing bandwidth use has increased 159.3% between 2010 and 2012.[1] In January 2013, worldwide, 432 million unique Internet users explicitly sought infringing content, 327 million of those unique Internet users being from North America, Europe, and Asia-Pacific.[2] While the accuracy of these numbers might be questioned,[3] there is no question that the amount of infringement—through the BitTorrent peer-to-peer file sharing system, through video streaming, through direct download cyberlockers, and through other file sharing networks—has increased exponentially worldwide over the last decade. Emblematic of efforts to respond to the spectacular increase in infringement is the *Viacom v. YouTube* lawsuit.[4]

For over seven years, media giant Viacom has been embroiled in a lawsuit against Internet juggernaut YouTube. Viacom owns hundreds of thousands of copyrighted works and has alleged that YouTube is liable for the copyright infringement of YouTube's subscribers. Specifically, Viacom claims that YouTube users upload and make available tens of thousands of YouTube videos that contain copyrighted material, constituting copyright infringement not only by the users, but also by YouTube, because YouTube is generally aware of and takes no action to prevent the infringement. Viacom alleges that it is losing hundreds of millions of dollars because of this infringement. YouTube has defended on the ground that the DMCA immunized YouTube from the infringing activities of its subscribers.

The 1998 DMCA was Congress' first legislative attempt to bring copyright law into the digital age. In an article written in 2009, Professor Ed Lee exclaimed that although ten years had passed since Congress enacted the DMCA, lingering questions remained about the DMCA's scope.[5] Five years later, in 2014, little has changed and those questions linger.

Perhaps the most pressing question is the one Professor Lee addressed in his article, and which the two above examples highlight: Does the DMCA immunize ISPs from all liability for subscribers' infringing conduct? While the DMCA contains a number of "safe harbors" that shield ISPs from certain

1. David Prince, *Sizing the Piracy Universe*, NETNAMES PIRACY ANALYSIS 1, 3 (Sept. 2013), https://copyrightalliance.org/sites/default/files/2013-netnames-piracy.pdf.

2. *Id.*

3. The report was commissioned by NBC Universal, a large media company, and thus, there is a strong chance the report is biased. *See id.* at 2.

4. Viacom Int'l, Inc. v. YouTube, Inc., 718 F. Supp. 2d 514 (S.D.N.Y. 2010).

5. Edward Lee, *Decoding the DMCA Safe Harbors*, 32 COLUM. J.L. & ARTS 233, 269 (2009).

forms of liability by adhering to certain procedures, less clear is whether falling within these safe harbors shields ISPs from all forms of liability, including secondary liability, e.g., vicarious and contributory liability. Although the Supreme Court has yet to weigh in, the structure of the DMCA and a number of recent decisions in the Ninth and particularly the Second Circuit Courts of Appeals have provided much clarity, finding that the DMCA does, in most cases, shield ISPs from secondary liability. But, a larger question looms. Assuming these courts are correct (a fair assumption), *should* ISPs nevertheless be responsible for preventing infringement occurring on their sites? As should be expected, there are conflicting views.

The DMCA was a grand bargain; it was a carefully crafted scheme balancing the interests of content providers (including independent artists like Mary Saint Francis and media companies and industries like Viacom, the Motion Picture Association of America and Recording Industry Association of America) and technology companies. The DMCA's balance is seen in three key parts. First, Sections 1201 and 1202 of the DMCA strengthened copyright holders' efforts to self-protect their works from unauthorized access and copying, using watermarking, encryption, and other technological protection measures ("TPMs"). Copyright holders needed legislative protection for TPMs because users would decrypt or otherwise circumvent the protection measures and then share with others their evasive methods. In an expensive cat and mouse game, content industries would then invest millions in new generation protection techniques, only to have those hacked within days of being introduced. The DMCA strengthened TPMs by making it illegal to (1) circumvent these protection measures and (2) traffic in devices used to circumvent TPMs.

The second key of the DMCA balance, Section 512, shielded ISPs[6] from liability if they fell within certain safe harbors and had neither actual knowledge of the infringing conduct nor were aware of any facts or circumstances from which infringing activity was apparent. This balance also included a "notice and takedown" procedure; in short, if copyright holders found infringing content on a website, the DMCA required them to send a notice to the ISP, which would then be required to take down the infringing content. The burden fell to copyright holders, not content hosts, to detect and enforce their rights.

---

6. Entities that provide services on the Internet include ISPs and Internet Access Providers, who provide services for accessing and using the Internet; Online Service Providers (OSP), who provide services on the Internet such as email, social media Web sites, as well as advertising services; and Web hosts, who provide space on servers for other clients to use. While there are differences in the type of services provided by these entities, throughout the article the term Internet Service Provider will be used unless there is a need to distinguish the entities.

The final piece of the DMCA balance was a firm admonition that ISPs were not required to affirmatively monitor their sites for infringing conduct. As such, ISPs could await notice from content providers and avoid liability for infringement by following the DMCA take down provisions.

As described, the twin aims of the DMCA balance was to provide meaningful protection for content providers, while also protecting ISPs from uncertain and crippling damages, which would curtail the development of the Internet.[7] Indeed, it is this aspect—encouraging the continued expansion and development of the Internet—that was at the heart of the DMCA.

While many have lauded the DMCA and its balance, there is little question that circumstances have changed since its passage in 1998, such that the balance is no longer as originally designed. According to Professor Lee, this is because the ISP safe harbors have eclipsed the other sections of the DMCA in importance.[8] That is an understatement. The anti-circumvention provisions have become all but meaningless, and the industry largely abandoned their use, as consumers revolted against TPMs because they were unwieldy and burdensome.[9] The grand bargain now looks like a really bad deal, at least for copyright holders, protecting content hosts more than the content owners themselves. Copyright holders have thus sought to "renegotiate" the DMCA by asking courts to interpret it more favorably towards them to effectuate

---

7. This characterization of the DMCA is not to suggest that others are not important in the calculus. Certainly, Internet users' rights and interests are important. So, too, are the interests of other industries, particularly the technology and software industries. The claim here, however, is not that these other interests are irrelevant, simply that at the time the DMCA was adopted, these interests did not play a significant factor. As discussed throughout the article, the DMCA is a series of compromises that sought to limit the liability of ISPs while addressing who should bear the burden associated with users' infringement.

8. *See* Lee, *supra* note 5, at 233 ("Today, it is increasingly clear that the safe harbors for ISPs have become the far more important part of the DMCA, particularly given the abandonment of Digital Rights Management ("DRM") in the music industry."). Professor Lee is surely right that the industry has relied significantly less on DRM/Technological Protection Measures ("TPM"), but one might legitimately question whether the industry has completely abandoned them. For example, the DVD Copy Control Association administers a regional playback control system. Under this system, copyright holders use technological protection measures to encode DVDs with regional codes, which limit the regions in which DVDs can be played. In particular, DVDs can be played only on DVD players that have the same regional code. Thus, for example, DVDs encoded as Region 3 are intended for use in Southeast Asia and will not play on DVD players encoded as Region 1, which covers the United States and Canada. The Blu-Ray Disc Association has also developed a similar regional coding standard for Blu-Ray discs. *See* ROBERT BRAUNEIS & ROGER SCHECHTER, COPYRIGHT: A CONTEMPORARY APPROACH 830 (2012). Despite this, there is little question that TPMs and DRM did not have the effect contemplated by the drafters of the DMCA.

9. Lee, *supra* note 5, at 233 n.3.

Congress' original intent and to restore balance. Throughout this Article, I refer to this interpretation as "DMCA-plus" or "DMCA 2.0."

Despite their pleas, the tide—and it is a strong one—is against imposing any additional obligation on ISPs to monitor their sites. Courts, scholars, and commentators all emphatically reject this notion.[10] Their reasons are compelling. The DMCA's balance has undeniably played an incredible role in the Internet's growth and development, and has also markedly contributed to innovation and the birth of related technologies and companies that might not otherwise have been developed. Altering the current balance might retard further development. Moreover, imposing additional liability on ISPs may be impractical and not technically feasible. ISPs are unable to discern from the millions of sites and posted content which material is infringing.[11] As argued, it is impossible for anyone other than the content owner to determine whether specific items are legitimately posted, even content owners themselves have trouble doing so. Courts and commentators also find this balance to be fair. As a policy matter, fairness demands that copyright owners, as the party with the greatest interest in protection, protect their own works, rather than having others police and enforce rights for them. This is particularly so given the considerable resources and costs associated with monitoring perhaps hundreds of millions of sites for content posted daily. Despite all of these creditable arguments, there are not insignificant arguments for an opposing view.

The 2014 Internet is not the same as the 1998 Internet. By some estimates, approximately every year since its creation, the Internet has doubled in size.[12] Contemplate this. It defies belief that in 1998, Congress (or any of the

---

10. *See* Jennifer L. Hanley, *ISP Liability and Safe Harbor Provisions: Implications of Evolving International Law for the Approach Set Out in* Viacom v. YouTube, 11 J. INT'L BUS. & L. 183, 186–89 (2012) ("Historically, domestic (and foreign) legislation has required ISPs to take a passive-reactive role in the battle against online copyright infringement . . . [and] the court in Viacom refused to place an affirmative burden on ISPs to police against copyright infringement . . . ."). I, too, am skeptical that copyright enforcement should be increased. *See generally* Donald Harris, *The New Prohibition: A Look at the Copyright Wars Through the Lens of Alcohol Prohibition*, 80 TENN. L. REV. 101 (2013).

11. *See, e.g.*, Lee, *supra* note 5, at 253 ("Congress realized that the question of what constitutes copyright infringement is often difficult, if not impossible, to determine outside of court. It sought to avoid creating perverse incentives that would turn ISPs into effective censors of material, indiscriminately removing vast amounts of content to avoid liability in the face of unclear legal standards. Accordingly, both the Senate and House committee reports indicate that the DMCA was drafted so as to avoid imposing a duty on ISPs to 'investigate possible infringements, monitor its service, or make difficult judgments as to whether conduct is or is not infringing.'") (quoting S. REP. NO. 105-190, pt. 2, at 32 (1998); H.R. REP. NO. 105-551(II), pt. 2, at 44 (1998)).

12. Annemarie Bridy, *Is Online Copyright Enforcement Scalable?*, 13 VAND. J. ENT. & TECH. L. 695, 697 (2011).

principals involved) envisioned such enormous growth (even while attempting to foster and encourage significant growth). As enormous and far-reaching as the Internet is, it continues to expand at a phenomenal rate. For the content industry, the most alarming aspect of the Internet's growth is the emergence of Web 2.0 and user-generated content, which allows users to upload, copy, distribute, and share content through decentralized servers on peer-to-peer networks.

To be sure, the Internet's growth has, as hoped, provided enormous rewards. People use the Internet as a vehicle to unearth previously undiscoverable works, to actively participate in creating cultural expression, to share interests, to explore, and ultimately to enjoy a fuller and more enriched life. The Internet has provided this and then some. The Internet's growth has also produced negative effects. As relevant here, the Internet has expanded exponentially the amount of copyright infringement occurring online. This was not unforeseen. In 1998, the Internet was already being used to reproduce and distribute infringing works. The DMCA was designed precisely to combat the infringement (although it seems improbable that the drafters could have forecast the magnitude of the infringement). The DMCA also provided certainty to ISPs regarding their liability. What was given up, however, was the ability of the law to accommodate changing norms and circumstances. In other words, without the DMCA, courts would necessarily develop liability rules to address Internet copyright infringement, which would evolve over time. Because the DMCA has frozen liability rules, a legitimate question is whether the change in circumstances necessitates a change in the DMCA.

This Article departs from literature supporting the current tide in subtle and not so subtle ways. The Article supports imposing liability against ISPs outside the DMCA's safe harbor provisions. This is the not so subtle departure. It is also controversial. The subtle shift, I hope, is a proposal that layers a duty-based regime over the already existing strict liability scheme. Under the duty-based regime, ISPs will be required to shoulder part of the burden of protecting content owners by taking reasonable efforts to prevent infringement. These efforts should include, at the very least, monitoring their sites using filtering technology to detect and prevent infringement. Even though several similar proposals have already been advanced,[13] as explained

13. *See* Brief for Audible Magic Corporation Neither Party at 15, Viacom Int'l, Inc. v. YouTube, Inc., 718 F. Supp. 2d 514 (2010) (Nos. 10-3270, 10-3342) [hereinafter Audible Magic Brief]; Note, *The Principles for User Generated Content Services: A Middle Ground Approach to Cyber-Governance*, 121 HARV. L. REV. 1387 (2008) [hereinafter *A Middle Ground Approach*]; *see also What is a Copyright Alert*, CENTER FOR COPYRIGHT INFORMATION (2014),

below, this proposal differs from those in a number of ways, including requiring cooperation from copyright holders, differentiating among ISPs, and rejecting strict liability in favor of a duty regime.

A number of grounds support such an approach. First, copyright secondary liability principles, including vicarious liability, are derived from employer-employee liability principles (in particular, respondeat superior). In employment law, particularly in the Title VII sexual harassment context, liability is contingent not only upon *remedial* measures taken by the employer/ISP to redress harassment/infringement, but also *preventative* measures designed to avert harassment/infringement. More specifically, in the Title VII sexual harassment context, an employer will be shielded from liability only if it both (1) takes measures to promptly address harassing behavior and (2) exercises reasonable care to prevent the behavior.[14] The DMCA scheme, as originally envisaged, followed this approach. The anti-circumvention and anti-trafficking provisions in Part I represented preventative measures designed to stop infringement from occurring. The Part II notice and takedown provisions represented remedial measures to correct infringement. Without the preventative measures, the scheme is unbalanced. Drawing, then, from employment law, requiring ISPs to monitor and block infringement restores the crucial balance.

A second ground supporting the proposal is that a reasonableness standard would not impose the same obligations on smaller ISPs as larger ones, and would therefore not erect substantial barriers for new entrants. Further, the proposal does not place the entire onus on ISPs. Rather, the system also requires copyright holders' cooperation. Duplicating regulations regarding border control measures for counterfeit copyrighted goods, copyright owners will be required to provide sufficient information to allow ISPs to detect infringement. Failing to do so would abrogate ISP duty.

For some ISPs, this will not affect a major change. For example, YouTube already monitors and filters for infringing content, using a proprietary Content ID system. In Viacom's copyright infringement suit against YouTube, because YouTube implemented this system, Viacom agreed to

---

http://www.copyrightinformation.org/the-copyright-alert-system/what-is-a-copyright-alert (last visited Nov. 11, 2015).

14. This is the *Ellerth/Faragher* affirmative defense. In companion cases, *Burlington Indus. v. Ellerth*, 524 U.S. 742 (1998), and *Faragher v. City of Boca Raton*, 524 U.S. 775 (1998), the Supreme Court set forth an affirmative defense for employers against vicarious liability. The defense comprises two necessary elements: (a) that the employer exercised reasonable care to prevent and correct promptly any sexually harassing behavior, and (b) that the plaintiff employee unreasonably failed to take advantage of any preventive or corrective opportunities provided by the employer or to avoid harm otherwise. *Ellerth*, 524 U.S. at 765; *Faragher*, 524 U.S. at 778.

limit its suit to infringing acts occurring before YouTube introduced its Content ID system.[15] This is the type of cooperative enterprise the proposal is aimed at achieving.

Part I of this Article traces the history of copyright's secondary liability. The history is brief, intending only to demonstrate the underpinnings of and reliance on employment law in designing comparable copyright principles. Part II will describe the DMCA. A full description of the DMCA has been provided elsewhere,[16] and this section will focus on illuminating the balance described above. Part III uses the *Viacom v. YouTube* case as a jumping-off point for analyzing the DMCA and for presenting opposing arguments regarding the Act's proper interpretation. As mentioned, Viacom sued YouTube arguing for a DMCA-plus interpretation and contending that YouTube should be held responsible for the copyright infringements committed by YouTube users whether or not YouTube fell within the DMCA's safe harbors. While this expansive interpretation is almost certainly wrong and has been, for the most part, rejected by the district court and the Second Circuit, the claims and defenses presented in the case provide fodder for arguments that liability should exist outside the DMCA safe harbors.

Part IV will identify and evaluate various commentators' proposals to impose ISP liability. The view in this Article is that these proposals reach too far, either because they threaten to erect substantial barriers for new entrants by requiring all ISPs to implement "the best technology available," or because they misread the DMCA as already providing for ISP liability.[17]

In the end, the question is not whether the proposed system is perfect. It is not. Rather, the question is whether the proposed system is better than the current one. More pointedly, will the costs and benefits of implementing the

---

15. Viacom Int'l, Inc. v. YouTube, Inc., 718 F. Supp. 2d 514 (S.D.N.Y. 2010).

16. *See generally* Richard Belsky, *The Digital Millennium Copyright Act and You: A Framework for a Functional Future*, 14 U. BALT. INTELL. PROP. L.J. 1, 5 (2005) (describing the history leading up to the DMCA's incorporation into the Copyright Act); Derek J. Schaffner, *The Digital Millennium Copyright Act: Overextension of Copyright Protection and the Unintended Chilling Effects on Fair Use, Free Speech, and Innovation*, 14 CORNELL J.L. & PUB. POL'Y 145, 146 (2004) (providing a summary of the DMCA and its legislators' intentions).

17. If not relying on the DMCA, some argue that existing law also compels ISP liability. For example, in their amicus brief, Intellectual Property and Internet Law Professors grounded their claims in ISPs being the "least cost avoider." *See* Brief for Intellectual Property and Internet Law Professors as Amicus Curiae Supporting Defendant-Appellee at 20–28, Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 20 (2d Cir. 2012) (Nos. 10-3270, 10-3342) [hereinafter Intellectual Property and Internet Law Professors Brief]. Whether ISPs are the least cost avoider is beside the point. Imposing liability is both fair and accords with congressional intent. Moreover, in contrast to the least cost avoider argument, this Article does not suggest that current law imposes liability, but rather argues that Congress might legislate to do so or that courts should do so.

new system outweigh the costs and benefits of the current scheme? Without empirical evidence regarding a host of factors, including (1) the cost to ISPs of acquiring and implementing filtering, blocking, or other technology; (2) the amount of infringement that will be prevented; and (3) the effect on current ISP business models and the resultant effect on consumers, among others, it is difficult to assess the wisdom of altering the current system. Moreover, the political will to engage in the fight for legislation may be lacking. After the failed SOPA and PIPA legislations, in which Congress sought to impose more stringent enforcement of online piracy, Congress may be less than willing to tackle copyright enforcement issues in the near future.[18] If left to the courts, I am less sanguine about change.

Nonetheless, if able to overcome these hurdles, serious thought ought to be given to a system that might better resolve the online infringement morass in which we find ourselves.

I. SECONDARY LIABILITY PRINCIPLES

A. Employment Law: Employer Liability for Supervisory Sexual Harassment

In 1998, in two groundbreaking decisions, *Faragher v. City of Boca Raton*[19] and its companion case, *Burlington Industries, Inc. v. Ellerth*,[20] the Supreme Court established a new standard for employer liability in sexual harassment cases. In the two cases, the Court held that employers can be liable for the acts of its supervisors if, for example, a supervisor harasses a subordinate employee. Under the *Ellerth/Faragher* framework, however, the employer may raise an affirmative defense to such liability. The affirmative defense consists of two elements: "(a) that the employer exercised reasonable care to prevent and correct promptly any sexually harassing behavior, and (b) that the plaintiff employee unreasonably failed to take advantage of any preventive or corrective opportunities provided by the employer or to avoid

18. Michael A. Carrier, *SOPA, PIPA, ACTA, TPP: An Alphabet Soup of Innovation-Stifling Copyright Legislation and Agreements*, 11 NW. J. TECH. & INTELL. PROP. 21, 21–23 (2013) (describing the proposed legislatives of SOPA and PIPA, which sought to protect copyright owners with broad guidelines). These legislations sparked online protests that included seven thousand websites shutting down. *Id.* This ultimately led Congress to shelve the legislation until issues that plagued the proposed bill are resolved. *Id.*

19. 524 U.S. at 775.

20. 524 U.S. 742 (1998).

harm otherwise."[21] An employer may further be strictly liable if the supervisor harassment is accompanied by an adverse official act (e.g., discharge, demotion, or undesirable reassignment).[22] The Court reasoned that creating the employer's affirmative defense provides an incentive for employers to take both preventive and remedial measures to limit occurrences of sexual harassment in the workplace.[23] Examples of such measures include instituting a grievance procedure, educating employees and supervisors about sexual harassment, and ensuring that employees are notified of their rights regarding harassment. While the contexts are obviously different, similar principles can be applied in the copyright context.

B. Copyright Law: Pre-DMCA Liability

ISP liability in the copyright context is primarily in the form of indirect infringement or secondary liability (as opposed to direct infringement). Secondary liability includes vicarious liability, contributory infringement, and inducement theories.

Copyright secondary liability concepts are an outgrowth of employment law liability standards. Two early Second Circuit cases, *Shapiro, Bernstein and Co. v. H.L. Green Co.*,[24] and *Gershwin Publishing Corp. v. Columbia Artists Management, Inc.*,[25] explicitly drew on agency principles of respondeat superior in expanding vicarious liability to copyright infringement. The Second Circuit held that "even in the absence of an employer-employee relationship one may be vicariously liable if he has the right and ability to supervise the infringing activity and also has a direct financial interest in such activities."[26] Contributory infringement "stems from the notion that one who directly contributes to another's infringement should be held accountable."[27] *Gershwin* again provides the classic statement of this doctrine: "[O]ne who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another, may be held liable as a 'contributory' infringer."[28]

---

21. *Faragher*, 524 U.S. at 778.
22. *Id.* at 808; *Ellerth*, 524 U.S. at 765.
23. *See*, *e.g.*, Petrosino v. Bell Atl., 385 F.3d 210, 226 (2d Cir. 2004).
24. 316 F.2d 304, 307 (2d Cir. 1963).
25. 443 F.2d 1159, 1162 (2d Cir. 1971).
26. *Id.*; *see also* Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259**,** 264 (9th Cir. 1996).
27. *Fonovisa*, 76 F.3d at 264.
28. *Gershwin*, 443 F.2d at 1162.

It was not long before these theories were being used against ISPs for providing services that subscribers used to infringe copyrighted works. These decisions were inconsistent, with some finding that ISPs satisfied the financial benefit and ability to control prongs of vicarious liability, while other courts held they did not.[29] As for contributory infringement, many courts found that ISPs either did not materially contribute to the infringement by merely providing online services, or that ISPs had insufficient knowledge of infringing conduct.[30] The inconsistent opinions resulted in uncertainty for ISPs, which also led to uncertainty regarding the potential growth of the Internet. Congress sought to eliminate this uncertainty with the Digital Millennium Copyright Act.

II. THE DIGITAL MILLENNIUM COPYRIGHT ACT

While the dilemma faced by content providers during the early stage of the digital era was users posting copyrighted content online, a drastic change occurred regarding Internet use; new technology allowed for peer-to-peer distribution of copyrighted content, and this new technology ushered in the rise of "user generated content," i.e., content, including videos, photos, and posts, that users had a hand in making. This change allowed for copyrighted material to be uploaded, copied, and distributed at a phenomenal rate. Liability issues arose. As one author put it:

> The emergence of Web 2.0 applications, such as UGC [user-generated content] sites, in 2004, complicated application of this regime in not fully anticipated ways. With users gaining the ability to upload, edit, and collaborate in information dissemination, webmasters came to be replaced by automated systems and the potential liability of OSPs became more uncertain.31

---

29. *Compare* A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1023 (9th Cir. 2001) (holding that Napster "financially benefits from the availability of protected works on its system"), *with* Ellison v. Robertson, 357 F.3d 1072, 1079 (9th Cir. 2004) (finding that AOL did not satisfy the direct financial benefit requirement for vicarious liability for copyright infringement).

30. *See* Newborn v. Yahoo!, Inc., 391 F. Supp. 2d 181, 190 (D.D.C. 2005) (holding that unauthorized third party use of trademarks allowed by Yahoo did not satisfy the knowledge requirement for contributory infringement); Monotype Imaging, Inc. v. Bitstream, Inc., 376 F. Supp. 2d 877, 889 (N.D. Ill. 2005) (finding that Bitstream's distribution of software did not demonstrate the requisite "purposeful, culpable expression and conduct" necessary to constitute contributory liability).

31. Martin B. Robins, *A Good Idea at the Time: Recent Digital Millennium Copyright Act § 512(c) Safe Harbor Jurisprudence Analysis and Critique of Current Applications and Implications*, 15 TUL. J. TECH. & INTELL. PROP. 1, 4 (2012).

One way in which content owners sought to address online infringement was to use Digital Rights Management ("DRM") and Technological Protection Measures ("TPMs"). DRM, such as digital watermarking, allowed owners to identify the copyright owner and aid them in tracking the source of redistributed copyrighted materials, while TPMs, such as password protected files and copy limit measures, allowed owners to prevent unauthorized copying and uses. During these early years, content owners/the media industry and users/software developers engaged in a cat and mouse game, in which software developers created and modified software that allowed more efficient and faster exchange of MP3 files, while the media industry sought ways to rein in such developments with DRM and TPMs.

No protection lasts forever; this is particularly so with regard to media technological protection measures. As fast as industry could develop protection measures, users would circumvent them. For example, on August 17, 1999, Microsoft released Windows Media 4.0, intended to be a secure format for music and other media files. On August 18, 1999, various Web sites offered a program that reportedly defeated the security features of Windows Media, stripping out the license information and making the files shareable.[32] Frustrated with the constant hacking, the media industry sought legislation to prevent circumvention of technological protection measures.

A. Part I—Preventative Measures

Preventing the circumvention of TPMs was seen as essential to protecting copyrighted materials in the digital age.[33] Accordingly, Congress enacted the DMCA, which included anti-circumvention provisions.[34] The DMCA went further than merely prohibiting circumvention of protection measures; it added *anti-trafficking* provisions. In particular, Section 1201(a)(1) governs "[t]he act of circumventing a technological protection measure put in place

32. THE SCI. & TECH. COUNCIL OF THE ACAD. OF MOTION PICTURE ARTS & SCIS., THE DIGITAL DILEMMA: STRATEGIC ISSUES IN ARCHIVING AND ACCESSING DIGITAL MOTION PICTURE MATERIALS (2007), http://www.cosmo-digital.com/cd2015/digital_dilemma.pdf.

33. *See* Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 304 (S.D.N.Y. 2000) ("Proponents of strong restrictions on circumvention of access control measures argued that they were essential if copyright holders were to make their works available in digital form because digital works otherwise could be pirated too easily.").

34. These provisions complied with the United States' international obligations under the World Intellectual Property Organization (WIPO) Copyright Treaty, which required member states to "provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights." Berne Convention for the Protection of Literary and Artistic Works, art. 11, Dec. 20, 1996, S. Treaty Doc. No. 99-27 (1986), 1161 U.N.T.S. 3.

by a copyright owner to control access to a copyrighted work." Section 1201(a)(2) prohibits creating and making available certain technologies that can be used to defeat technological protections against unauthorized access to a work. It provides: "No person shall . . . offer to the public, provide, or otherwise traffic in any technology . . . that is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under [the Copyright Act]."[35]

B. Part II—Remedial Measures

The DMCA's remedial provisions involve so-called "safe harbors." These are contained in Section 512 of the Copyright Act. While there are five safe harbors, two are important here. Under Section 512(c), ISPs are not liable for hosting or storing material that is posted by or at the direction of users.[36] An ISP is immune from liability, however, only if it (1) has no actual knowledge that the material is infringing; (2) is not aware of any facts or circumstances from which infringing activity is apparent (so-called "red flag knowledge,"

---

35. 17 U.S.C. § 1201 (2015). Other requirements of the anti-trafficking section are laid out in § 1201(a)(2)(B) ("No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title.") and § 1201(a)(2)(C) ("No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that is marketed by that person or another acting in concert with that person with that person's [sic] knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.").

36. In full, 17 U.S.C § 512(c) (2012) provides:

Information residing on systems or networks at direction of users. ― (1) In general. ―A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider, if the service provider―

(A)(i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing;

(ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or

(iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;

(B) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and

(C) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.

also considered constructive knowledge);[37] (3) removes infringing material when it becomes aware of the infringement; and (4) if the ISP receives a financial benefit directly attributable to the infringement, it must not have the right and ability to control the infringement.

Section 512(d) immunizes ISPs that provide information location tools (e.g., hypertext links) that link users to online locations that contain infringing material. As with Section 512(c), ISPs are immune from liability only if they do not have actual or red flag knowledge, and remove the infringing material upon obtaining knowledge of it, and also receive no financial benefit while having the right and ability to control the infringement.[38]

Finally, Section 512(m) is clear that ISPs have no duty to monitor. That section provides that the previous sections are not conditioned on a service provider monitoring its service or "affirmatively seeking facts indicating infringing activities."[39]

---

37. *See* David Post, *Viacom v. YouTube, and Why it Matters*, VOLOKH CONSPIRACY (July 19, 2010, 11:34 AM), http://www.volokh.com/2010/07/19/viacom-v-youtube-and-why-it-matters/ (discussing a case in which a judge found content titled as "illegal" was not considered a "red flag" because of the nature of the website).

38. 17 U.S.C. § 512(d) (2012) ("Information location tools. —A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider referring or linking users to an online location containing infringing material or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hypertext link, if the service provider—

(1)(A) does not have actual knowledge that the material or activity is infringing;

(B) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or

(C) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;

(2) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and

(3) upon notification of claimed infringement as described in subsection (c)(3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity, except that, for purposes of this paragraph, the information described in subsection (c)(3)(A)(iii) shall be identification of the reference or link, to material or activity claimed to be infringing, that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate that reference or link.")

39. *Id.* § 512(m) provides:

Protection of Privacy**.** —Nothing in this section shall be construed to condition the applicability of subsections (a) through (d) on— (1) a service provider monitoring its service or affirmatively seeking facts indicating infringing activity, except to the extent consistent with a standard technical measure complying with the provisions of subsection (i); or (2) a service provider gaining access to, removing, or disabling access to material in cases in which such conduct is prohibited by law.

Despite new legislative protection, the anti-circumvention provisions quickly lost their intended value as users revolted against TPMs. For one, the measures made it more difficult to use devices.[40] The cumbersome nature of the content protection design discouraged use of these devices and pushed consumers to devices and works that did not contain such measures. Consumer dissatisfaction also centered on the inability to use legally purchased music on different devices. In short time, TPMs were seen as a failure and the media industry all but abandoned such use.[41]

Without the benefit of DRM/TPM protection, and the lack of duty for ISPs to monitor content, copyright owners sought a different measure of protection—the DMCA-plus/DMCA 2.0. More particularly, copyright holders sought protection under theories of ISP indirect infringement beyond the DMCA safe harbors. This should come as no surprise. Indirect liability is the "standard legal response" where direct liability will be ineffective, such as when the relevant direct actors are not subject to effective reach of the law, and where the direct actors cannot use contract law to shift responsibility.[42] Indirect liability is also appropriate when one party is in a position to detect and deter the direct actor's bad acts, such as in the employer-employee context.[43] Here, the difficulty of identifying and suing the thousands of infringing subscribers, and that the subscribers may be judgment proof with regard to large damage awards even if identified and successfully sued, arguably places them effectively beyond the reach of the law. Indeed, copyright holders tried unsuccessfully to pursue direct actions against individuals. Over the last decade, in an effort to combat rampant music piracy, the recording industry sued tens of thousands of individual infringers.[44] The industry soon realized that the suits were an inefficient and ineffective means to stem the tide of piracy, as suing thousands for infringement of millions had little effect on copyright holder's bottom line, and the suits backfired miserably, resulting in a public relations nightmare. Beyond the difficulty of suing subscribers, indirect liability seemed

---

40. *See, e.g.*, Kristin R. Eschenfelder, *Digital Rights Management Could Threaten Academic Research*, N.Y. TIMES (Oct. 10, 2012), www.nytimes.com/roomfordebate/2012/10/10/does-the-law-support-inventors-or-investors/digital-rights-management-could-threaten-academic-research.

41. *See, e.g.*, David Kravets, *DRM is Dead, But Watermarks Rise from the Ashes*, WIRED (Jan. 11, 2008), http://archive.wired.com/entertainment/music/news/2008/01/sony_music.

42. *See* Doug Lichtman & Eric Posner, *Holding Internet Service Providers Accountable*, 14 SUP. CT. ECON. REV. 221, 223, 229–30 (2006); *see also* Alan O. Sykes, *The Economics of Vicarious Liability*, 93 YALE L.J. 1231, 1236–38 (1984).

43. Lichtman & Posner, *supra* note 42, at 230.

44. *See* Harris, *supra* note 10, at 102 (discussing how the copyright war is "a battle for control over copyright's future").

particularly appropriate because ISPs are in a position to detect and deter subscriber misconduct. As such, with the ever-growing incidents of infringement, and left with few other options, it was reasonable to expect Viacom to turn to YouTube and other ISPs as responsible parties under indirect liability theories. Getting past the DMCA, however, would prove challenging, if not impossible.

III. VIACOM V. YOUTUBE: INTERPRETING THE DMCA AND DEFINING ISP LIABILITY

There have been few appellate cases interpreting the DMCA and its safe harbor provisions.[45] *Viacom v. YouTube* is one such case, and the saga provides a useful vehicle to discuss the various contentions of the content industry and ISPs, and also to interpret key DMCA provisions.[46]

In March of 2007, Viacom, along with a number of its subsidiaries, brought suit against YouTube and Google, Inc., alleging that YouTube should be liable for subscribers' infringement, and seeking a permanent injunction requiring YouTube to employ reasonable methodologies to prevent or limit infringement.[47] Viacom alleged three indirect liability theories: inducement, vicarious liability, and contributory infringement.[48] According to Viacom, YouTube had full knowledge of the copyrighted nature of tens of thousands of videos on the site, and promoted itself as a vehicle for infringement.[49] Viacom further alleged that YouTube's then-policy of providing improved infringement detection services to those copyright owners who had content licenses with Google, coupled with YouTube's ineffective responses to DMCA takedown notices, and YouTube's own policing of users who make unauthorized uses of YouTube created a right and ability to control infringing conduct.[50] Each party moved for summary judgment; the district court granted YouTube's motion.[51]

The court held that the DMCA did not require YouTube to affirmatively monitor its site for infringing conduct and material.[52] The court correctly

45. *See* Viacom Int'l, Inc. v. YouTube, Inc., 718 F. Supp. 2d 514 (S.D.N.Y. 2010); UMG Recordings, Inc. v. Veoh Networks, Inc., 665 F. Supp. 2d 1099 (C.D. Cal. 2009), *aff'd*, 718 F.3d 1006 (9th Cir. 2013).

46. *Viacom*, 718 F. Supp. 2d at 514.

47. *Id.* at 516.

48. *Id.*

49. *Id.* at 518.

50. *Id.* at 516.

51. *Id.* at 529.

52. *Id.* at 523.

noted that the DMCA squarely placed this burden on the copyright holder, and found that the DMCA takedown process was appropriate and efficient.[53] Absent actual or red flag knowledge, the court stated, Viacom had the burden of identifying specific infringement, regardless how ubiquitous the infringement may be.[54] The court also dismissed Viacom's claim that YouTube's behavior fell outside of §512(c) protection.[55] The court found where there is no "item-specific" knowledge of infringement, ISPs cannot have the "right and ability to control" necessary to disqualify DMCA protection under § 512(c)(1)(B).[56]

The court interpreted the actual and red flag knowledge elements as requiring "knowledge of specific and identifiable infringements of particular individualized items."[57] In other words, "generalized knowledge" of infringing activity—even if there were general knowledge of millions of infringing activity—was insufficient to create liability for YouTube and afforded YouTube safe harbor protection.[58]

On appeal, the Second Circuit affirmed the district court's holding that actual or "red flag" knowledge required knowledge of "specific and identifiable instances of infringement."[59] However, it concluded the district court erred in assuming a reasonable jury could not find YouTube had that knowledge.[60] The Second Circuit agreed that the DMCA does not require ISPs to actively monitor sites for infringement.[61] Unlike the district court, the Second Circuit held that a host need not have item-specific knowledge of infringement in order to control the infringement.[62] The Second Circuit made clear, however, that the ability to remove or block access to materials posted on a website is insufficient to satisfy the control element; the court was less

53. *Id.* at 524.
54. *Id.* at 525.
55. *Id.* at 529.
56. *Id*. at 527.
57. *Id.* at 523.
58. *Id.* at 523–25.
59. Viacom Int'l, Inc. v. YouTube, Inc. 676 F.3d 19, 31 (2d Cir. 2012) (explaining that actual knowledge referred to actual knowledge as a *subjective* standard whether an ISP subjectively knew about infringement, whereas "red flag" knowledge refers to a subjective awareness of facts that made specific infringement "'*objectively'* obvious to a reasonable person");
60. *Id.* at 26.
61. *Id.* at 35.
62. *Id.* at 42.

clear about what was actually required, stating merely that what was required was "something more."[63]

Because the district court had not adequately considered Viacom's evidence that YouTube was willfully blind to the infringements, the appellate court reversed summary judgment.[64] The Second Circuit held that even though the DMCA does not mention willful blindness, the DMCA allowed for willful blindness "in appropriate circumstances" to show knowledge or awareness of specific infringements.[65] On remand to the district court, the parties' new summary judgment motions centered around four specific issues: (1) YouTube's knowledge or awareness of specific infringements, (2) YouTube's willful blindness, (3) if YouTube had a "right and ability to control" infringing activities under § 512(c)(1), and (4) whether YouTube's conduct of syndicating works to third parties fell within the safe harbor of § 512(c).[66]

On remand, the district court again found for YouTube, granting its renewed motion for summary judgment.[67] According to the court, Viacom failed to produce evidence of willful blindness,[68] and Viacom had not demonstrated the "something more" required for § 512(c)(1)(B)'s "right and ability to control."[69] The court defined "something more" as requiring YouTube to influence or participate in the infringement.[70] This is satisfied by "high levels of control," "purposeful conduct" or direct involvement with the infringing activity.[71] Because Viacom failed to prove any of these, the court held that YouTube was shielded by the DMCA safe harbor.[72]

---

63. *See id.* at 38. The court had difficulty defining "something more," stating: "The remaining—and more difficult question—is how to define the "something more" that is required." *Id.* (providing a number of examples such as whether the ISP induced infringement and whether the ISP "used a monitoring program to prevent users from certain activities").

64. *Id.* at 41–42. The court explained that willful blindness could take an ISP out of the safe harbor protections, and defined willful blindness as being "aware of a high probability of the [infringement] and consciously avoid[ing] confirming that fact." *Id.* at 25 (citation omitted).

65. *Id.* at 35.

66. Viacom Int'l, Inc. v. YouTube, Inc. 940 F. Supp. 2d 110, 113 (S.D.N.Y. 2013).

67. *Id.* at 123.

68. *Id.* at 116–17.

69. *Id.* at 119–22.

70. *Id.* at 118.

71. *Id.*

72. *Id.* at 119, 121–22. The court found that the lack of monitoring for infringement, enforcement of basic content rules, facilitating access to all user-stored material regardless whether it was infringing, and monitoring for some infringing material all constituted DMCA protected actions. *Id.* The court further determined that the final issue on remand, whether third party syndication constituted protected actions under § 512(c), was found to be a repackaging of technological functions already ruled to be protected by the district court. *Id.* Though YouTube

Viacom again appealed. Viacom argued that the district court failed to adhere to the Second Circuit's "right and ability to control" holding, and that YouTube exhibited such control by inducing users to infringe.[73] Viacom argued that YouTube's entire business was founded on the "major lure" of "blatantly illegal" clips, which constituted inducement.[74] Viacom further argued that YouTube had both actual knowledge and red flag knowledge (i.e., awareness of facts and circumstances) and had been willfully blind, arguing that YouTube's awareness of a high probability of infringement coupled with a deliberate effort to avoid learning of specific infringements satisfied the standard.[75] After the appeal was filed, and after spending millions of dollars litigating the suit, the parties settled.[76] Both parties have been silent about the settlement terms, which have not been publicly disclosed.

There are a number of important takeaways from the *Viacom* dispute. First, the DMCA prohibits courts from requiring ISPs to actively monitor for infringement.[77] ISPs can await notice from copyright holders before taking remedial action, unless ISPs otherwise have knowledge of infringement.[78] Second, the knowledge required for ISP action is knowledge of specific instances of infringement.[79] Thus, even though YouTube may have generalized knowledge that rampant infringement exists on its site, it has no duty to take any action. Third, if ISPs fall within the DMCA safe harbor provisions, they will not be liable under indirect liability theories of vicarious and contributory infringement; inducement liability, however, may still lie.[80] The hurdles thus posed by the DMCA, as interpreted by the Second Circuit, are extremely high. Are they justified?

---

did manually select content for one license deal, this was the sole example and only occurred to better ease the transmission of content between YouTube and the licensee. *Id.* Finally, the court found that the syndications were to provide access to material stored at the discretion of users. *Id.*

73. Opening Brief for Plaintiffs-Appellants at 32, Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19 (2d Cir. 2012) (No. 13-1720), 2013 WL 3964710, at *24–*25.

74. *Id.* at *25.

75. *See id.* at *25–*26 (explaining that Viacom argued that the district court improperly shifted the balance of proof in the determining knowledge, as YouTube should sustain the burden of proving its own affirmative defense of DMCA safe harbor).

76. Viacom Int'l, Inc. v. YouTube, Inc., 940 F. Supp. 2d 110, No. 13-1720 (S.D.N.Y. Mar. 19, 2014), *appeal withdrawn*, (revealing that as of March 19, 2014, Viacom has terminated an appeal that was initiated on May 5, 2013).

77. *See* Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 35 (2d Cir. 2012).

78. *See id.* at 37.

79. *See id.* at 41.

80. *See id.* at 37–38.

IV. PROPOSALS TO IMPOSE LIABILITY ON ISPS

Many praise the DMCA and applaud the Second Circuit's opinion limiting ISP liability. For example, Professors Annemarie Bridy and David Post authored an amicus brief filed in the *YouTube* case and signed by forty other law professors in which they exclaim that "[o]ver the last decade, the scheme that Congress implemented in the DMCA . . . has been resoundingly, and perhaps even remarkably, successful at forging an equitable balance among [] conflicting interests."[81] Similarly, Fred von Lohmann, senior copyright counsel at Google, recently said on behalf of Google that "[w]e believe that the time-tested [DMCA] 'notice-and-takedown' process for copyright strikes the right balance between the needs of copyright owners, the interests of users and our efforts to provide a useful Google Search experience."[82] These folks would resist efforts to alter the current DMCA structure and balance despite the significant changes since the passage of the DMCA and the meteoric rise in infringement. They would contend that copyright holders, not ISPs, should be responsible for monitoring and detecting infringement and that ISPs should bear little to no responsibility beyond the DMCA, so as to continue the enormous growth of the Internet.

The DMCA and the current ISP liability scheme are not without its critics, however. Some express concern about the DMCA's ambiguities (such as whether indirect liability and inducement should apply),[83] some also question whether the DMCA encourages rather than discourages infringement. Most forcefully, Professors Helman and Parchomovsky argue that the DMCA's structure inappropriately places too much of the enforcement responsibility on copyright owners, even though ISPs are in the best position to deter

---

81. *See* Intellectual Property and Internet Law Professors Brief, *supra* note 17, at 3.

82. *See* David Goldman, *Google Kills 250,000 Search Links a Week*, CNN MONEY (May 24, 2012, 3:23 PM), http://money.cnn.com/2012/05/24/technology/google-search-copyright ("Moreover, there is little question that ISPs rely on the safe harbors. As one commentator observed: 'Many Web site operators in this space rely heavily upon the terms of this safe harbor as a foundation of their business model. The author, in his practice, has observed numerous firms with major interactive Web presences, who are not only cognizant of the provision's terms, but make every effort to comply with its letter and spirit as a fundamental part of their risk management effort.'").

83. Lee, *supra* note 5, at 260; Lital Helman & Gideon Parchomovsky, *The Best Available Technology Standard*, 111 COLUM L. REV. 1194, 1207 (2011) ("As a result of the ambiguity in section 512(c), services can never be certain that they are really protected from vicarious liability or from claims of inducement—a vague doctrine in and of itself—even if they comply with all the statutory criteria that qualify one for the safe harbor."); Robins, *supra* note 31, at 4.

infringement.[84] They also contend that the DMCA's failure to mandate that ISPs monitor their sites and/or filter content for infringement provides a disincentive to innovate in filter technology.[85] As discussed below, they propose a new liability scheme.

Law professors Ronald Cass, Raymond Nimmer, and Stuart N. Brotman also attack the DMCA, arguing that the restrictive reading of the DMCA improperly immunizes parties best able to prevent, limit, or eliminate harm.[86] In seeking a DMCA-plus type interpretation, these professors rely on the "least cost avoider" or "most efficient risk bearer" principles in demanding ISPs take reasonable precautions.[87] Reasonableness "turns mainly on the cost-effectiveness of the precautions."[88] Because their proposed liability pivots on cost-effectiveness, "[i]ndividuals are not required to take precautions that cost more than the value of the harms the precautions can be expected to prevent, nor are they required to take precautions when another individual can prevent the same harm at far less cost."[89] These principles apply with stronger force when direct deterrence is impracticable, such as when it becomes prohibitively expensive to identify and pursue direct infringers.[90] The authors conclude that "[w]hile there may be no general monitoring requirement imposed under the law, an entity that is aware it is facilitating substantial amounts of infringement and ignores cost-effective means for limiting those infringements generally will be deemed a contributory infringer," and should fall outside the DMCA's safe harbor.[91]

Finally, Professors Mehra and Trimble argue that while the DMCA's safe harbor provisions greatly benefit ISPs, the provisions unfairly solidify existing ISP market position.[92] This, in turn, hampers the entry of new service providers into the market, which retards technological progress and harms

84. *See* Helman & Parchomovsky, *supra* note 83, at 1208–09 ("An additional concern emanating from the present regime, which places enforcement in the hands of copyright owners, is that too much speech will be curtailed.").

85. Helman & Parchomovsky, *supra* note 83, at 1202.

86. *See* Brief for Stuart N. Brotman, Ronald A. Cass, and Raymond T. Nimmer as Amici Curiae Supporting Plaintiffs-Appellants at 13–14, Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19 (No. 10-3270).

87. *Id.* at 3.

88. *Id.* at 5.

89. *Id.*

90. *Id.* at 6.

91. *Id.* at 17.

92. *See* Salil K. Mehra & Marketa Trimble, *Secondary Liability, ISP Immunity, and Incumbent Entrenchment*, 62 AM. J. COMP. L. 685, 685 (2014).

society.[93] In light of these criticisms, a number of proposals have been advanced to augment the DMCA safe harbor provisions.

A. Best Technology Available

Helman and Parchomovsky advocate imposing a monitoring duty on ISPs to prevent infringement.[94] Their ex ante regulation would require ISPs to use the "best technology available" to monitor and filter infringing material.[95] Specifically, under their proposal, ISPs would filter content before posting and would compare the content against a massive copyright database containing metadata and digital "fingerprints" provided by copyright owners to identify their works.[96] This preventative measure would not replace the remedial measure of the notice and takedown procedures, but rather would complement it. Their proposal would make filtering of uploaded content a prerequisite for DMCA safe harbor protection.[97] To protect against prohibitive expense and unfairness to new or smaller ISPs, the authors propose that a third party handle the filtering and monitoring duties for all ISPs; this would allow for economies of scale that would reduce the costs for all ISPs.[98]

B. Economic Safe Harbor

Another proposal is an "opt-in regulatory regime," under which ISPs could decide to opt in to a filtering and monitoring system that also would compare user content to a database of copyrighted material (administered by the U.S. Copyright Office).[99] Upon finding a "match," the copyright holder could choose among four options: (1) have no action taken, (2) receive notice that a match has occurred, (3) require an advertisement for the original material

---

93. *See id.* at 705 ("[A]n underappreciated aspect of these three regimes is the degree to which they may tend to benefit incumbent firms and ossify the development of Internet services."); *see also* Lichtman & Posner, *supra* note 41, at 224–25 (advocating for ISP liability for "Internet pests," i.e., worms, viruses, and other forms of malicious computer code introduced into the system by users).

94. *See* Helman & Parchomovsky, *supra* note 83, at 1214 ("Webhosts, for their part, should be entrusted with the tasks of screening for infringing material and preventing it from being posted if it matches copyrighted works in the database.").

95. *Id.* at 1212.

96. *Id.* at 1214.

97. *Id.* at 1217.

98. *Id.* at 1215.

99. *See* Bryan E. Arsham, *Monetizing Infringement: A New Legal Regime for Hosts of User-Generated Content*, 101 GEO. L.J. 775, 792 (2013).

be displayed with the user-generated content, or (4) require payment for use of the work.[100] Importantly, the copyright owner would not have the ability to remove the infringing content.[101] As such, any required payment would constitute a compulsory royalty, which under this scheme would be set by the government and would both be small and apply only to uploaded content ("in order for it to be economically feasible for websites to adopt this safe-harbor provision.")[102] ISPs that opt in to this regime would be shielded from liability, outside the DMCA notice and takedown provisions.[103] The purported benefits of this regime are that it would protect ISPs from legal uncertainty and high legal costs, while at the same time providing copyright holders with remuneration for the downloading of their copyrighted content.[104]

C. Market Responses –Filtering; UGC Principles; YouTube's Content ID System, and the Copyright Alert System

Other solutions involve market participants, i.e., ISPs, consumers, and copyright owners, resolving the issues amongst themselves, without the need for further regulation or oversight.[105] The ability for market participants to react more quickly to changes in business models, technological developments, and consumer attitudes counsel for such self-governance and private arrangements. Three arrangements are described here.

---

100. *Id.* at 792–95.
101. *Id.* at 799.
102. *Id.* at 794.
103. *Id.*
104. *Id.* at 795–98.
105. The view that online activities should be subjected to limited or no government regulation is not new. *See, e.g.*, David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1370 (1996) ("[T]he Net can develop its own effective legal institutions."); *see* Lawrence Lessig, *The Limits in Open Code: Regulatory Standards and the Future of the Net*, 14 BERKELEY TECH. L.J. 759 (1999); Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553, 580–81 (1998); *see also* Llewellyn Joseph Gibbons, *No Regulation, Government Regulation, or Self-Regulation: Social Enforcement or Social Contracting for Governance in Cyberspace*, 6 CORNELL J.L. & PUB. POL'Y 475 (1997); *cf.* Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199 (1998); Jack Goldsmith, *Regulation of the Internet: Three Persistent Fallacies*, 73 CHI.-KENT L. REV. 1119 (1998).

1. UGC Principles

The first of these efforts was spurred by cooperative efforts between media and technology companies.[106] On October 18, 2007, major players in the media industry (CBS, Fox, NBC, Universal, and Viacom) and the Internet industry (MySpace and DailyMotion) negotiated an agreement to curb online infringement entitled "Principles for User Generated Content Services" ("UGC Principles" or "Principles").[107] The Principles provide guidelines and a legal framework that govern user-uploaded and user-generated audio and video content while protecting intellectual property rights.[108] The Principles require ISPs to use filtering technology to block content that matches copyrighted material submitted by copyright owners to a back-end database (similar to the clearinghouse proposed in the *Best Technology* article). As such, the Principles protect media interests by eliminating infringing material on host sites, along with protecting user privacy interests and user's ability to use copyright works for fair use.[109] Copyright owners agree not to sue ISPs if ISPs follow the guidelines.[110]

Thus, despite no legal obligation to do so, some ISPs have been using filtering technology, including methods such as watermarking, fingerprinting, and YouTube's proprietary Content ID (below).[111] While not a direct result of the UGC Principles—after all, the technologies have existed in some form since 2004—some have claimed that the fingerprinting envisioned by the UGC Principles "has become an industry standard among both copyright holders and UGC sites."[112] Audible Magic, for example, is a leading developer of filtering technology, providing this technology to copyright owners to send information ("fingerprints") to ISPs.[113] That information is then submitted to an expansive database that contains copyrighted material that is fingerprinted, i.e., identified using information as

106. *See, e.g.*, *A Middle Ground Approach*, *supra* note 13.

107. PRINCIPLES FOR USER GENERATED CONTENT SERVICES, http://www.ugcprinciples.com (last visited Sept. 25, 2014).

108. *See* Audible Magic Brief, *supra* note 13, at 15 (explaining UGC Principles).

109. *See A Middle Ground Approach*, *supra* note 13, at 1400.

110. *Id.* at 1405.

111. *See* Audible Magic Brief, *supra* note 13, at 8.

112. *See* Lauren G. Gallo, *The (Im)possibility of "Standard Technical Measures" for UGC Websites*, 34 COLUM. J.L. & ARTS 283, 285 (2011) (listing various companies that develop and use fingerprinting technology including Viacom (Auditude), Audible Magic, and MotionDSP); *see also A Middle Ground Approach*, *supra* note 13, at 1400 (citing Justin D. Fitzdam, Note, *Private Enforcement of the Digital Millennium Copyright Act: Effective Without Government Intervention*, 90 CORNELL L. REV. 1085, 1087 (2005)).

113. *See* Audible Magic Brief, *supra* note 13, at 7.

tempo, tone, pitch, and color (depending upon the content).[114] The system uses an algorithm that compares the fingerprints with works on the site, filtering matches.[115] When the system finds a match, the ISP prevents the uploading of the material.[116]

2. Content ID

Being a voluntary agreement, the UGC Principles suffered from the absence of key players. YouTube was the most notable holdout.[117] YouTube instead created its own monitoring and filtering system, the Content ID system. Content ID works similar to other fingerprinting technology.[118] It allows copyright owners to send YouTube copyright information, which is then submitted to a database.[119] The Content ID system compares the fingerprints with works on the site, and identifies matches. As with the UGC Principles, identified matches are prevented from being uploaded to, or are removed from, the site.

3. Copyright Alert System

The Copyright Alert System ("CAS," also known as "six strikes") is another self-governance mechanism to curb online infringement.[120] As countries have done,[121] media and Internet giants[122] have created a privately

---

114. Gallo, *supra* note 112 at 285.

115. There are other filtering technologies. Veoh, for example, uses "hash filtering" software, "which identifies videos that are identical to any videos that have already been taken down as allegedly copyright infringing and blocks any duplicates that users may attempt to upload." Mehra & Trimble, *supra* note 92, at 692.

116. Mehra & Trimble, *supra* note 92, at 691–92.

117. *See* Arsham, *supra* note 99, at 791.

118. *Id.*

119. *Id.*

120. Professors Mehra and Trimble question whether the CAS is truly self-regulation. They note: "Though presented as a form of self-regulation, the CAS seems in part a product of informal guidance by government officials. The Governor of New York, Andrew Cuomo, facilitated the negotiations, and the Obama Administration endorsed the plan, reportedly after Justice Department officials informally vetted the program. Notably, although the Justice Department (and the FTC as well) provides formal guidance through its business review letter program, the firms involved did not seek such formal review." Mehra & Trimble, *supra* note 92, at 703.

121. *See infra* Section V.

122. The negotiating parties look like a who's who in their respective industries, which include: "Independent Film and Television Alliance (IFTA) and the American Association of Independent Musicians (A2IM); Recording Industry Association of American members Universal Music Group, Warner Music Group, Sony Music Entertainment, and EMI Music;

governed "graduated response" system. Under the system, ISPs first notify subscribers that their accounts have been used to infringe copyrights; if the conduct continues, ISPs take subsequent action, including requiring some form of subscriber acknowledgement that notice has been received, and then "mitigation measures," which may consist of "temporary reductions of Internet speeds, redirection to a landing page until the subscriber contacts the ISP to discuss the matter or reviews and responds to some educational information about copyright, or other measures that the ISP may deem necessary."[123] The graduated response system is an ex post measure that keeps the burden on the content owner to notify an ISP of suspected infringement, after which the ISP sends the action letters to the subscriber.

D. Shortcomings of the Proposals

Because all of the ex ante systems rely on current filtering technology, they all suffer from criticisms relating to the limitations of the technology. More specifically, some have questioned the technology's lack of "reliability" and "verifiability."[124] The system may not detect infringing content (false negatives) and may produce matches that are not infringing (false positives).[125] Moreover, as Professors Katyal and Schultz note, the technology is unable to distinguish from unauthorized use and licensed use,

---

Motion Picture Association of America members Walt Disney Studios Motion Pictures, Paramount Pictures, Sony Pictures Entertainment, Twentieth Century Fox Film Corporation, Universal Studios, and Warner Brothers Entertainment; and the ISPs AT&T, Cablevision, Comcast, Time Warner Cable, and Verizon." Mehra & Trimble, *supra* note 92, at 703.

123. *Id.* at 704 (citations omitted) ("Finally, if the behavior continues, and the ISP did not institute a mitigation measure after the fifth alert, it must send a sixth alert and implement such a measure. A user who disagrees with the CAS allegations may, at some expense, seek a hearing before American Arbitration Association (AAA) affiliated reviewers; users may only challenge a determination based on one of six pre-defined grounds, including unauthorized use, fair use and public domain due to publication prior to 1923. Given repeat player effects and the fact that AAA works for the operator of the CAS, the Center for Copyright Information (CCI), which was founded for the benefit of copyright holders, the review does not seem likely to guarantee impartiality."); *see also What is a Copyright Alert?*, CTR. FOR COPYRIGHT INFORMATION, http://www.copyrightinformation.org/the-copyright-alert-system/what-is-a-copyright-alert (last visited Oct. 15, 2015) (explaining the functionality of the CAS).

124. Viacom Int'l, Inc. v. YouTube, Inc., 718 F. Supp. 2d 514, 528 (S.D.N.Y. 2010).

125. According to Audible Magic, their current technology achieved 99% correct identifications on files along with a false positive rate that is approximately 1 in 10,000 Audible Magic Brief, *supra* note 13, at 16. Audible Magic also claims that it constantly updates its database, so that it is as up-to-date as possible. *Id.* at 18.

and from infringing use and noninfringing fair and tolerated uses.[126] Even though Helman and Parchomovsky claim that the technology will filter mostly verbatim uses,[127] Katyal and Schultz counter that even 100% verbatim uses that are noninfringing "abound," cataloguing various court opinions supporting the contention.[128]

Katyal and Schultz continue their spirited attack on filtering technology models (primarily the Best Technology model) contending that ex ante filtering and blocking results in unconstitutional prior restraints. They make a compelling case, noting that rather than keeping an allegedly infringing work up until a complaint is made, the ex ante nature of the filtering systems prevents the work from being posted. Even a system that allows for immediate review will be inadequate to address the prior restraint of time-sensitive noninfringing uses.[129]

Katyal and Schultz also question the wisdom of choosing to support a filtering technology industry that is as yet underdeveloped and unproven, while undermining support for an ISP industry that has been "proven drivers of economic growth."[130]

The proposals have other limitations. As acknowledged by the article's author, the Economic Safe Harbor's limitations include: (1) copyright holders would be unable to remove infringing works from these websites—instead opting for a royalty; (2) the system results in significant and prohibitive costs; (3) false matches would result in unwarranted royalties; (4) the system might actually lead to more widespread infringement; and, most importantly, (5) in practice, the system may prove ineffective.[131] A major criticism of the CAS is that it fails to represent user interests, as it is exclusively an agreement between media and ISPs. Here, Mehra and Trimble caution:

> [T]he creation of a system impacting users' rights through the cooperation of competitors and industry partners creates concern that the interests of consumers and of nascent competitors may be

126. Sonia Katyal & Jason Schultz, *The Unending Search for the Optimal Infringement Filter*, 112 COLUM. L. REV. SIDEBAR 83, 103 (2012).

127. Helman & Parchomovsky, *supra* note 83, at 1229–30.

128. Katyal & Schultz, *supra* note 126, at 98–99.

129. *See, e.g.*, Mark Glaser, *Fake Anchor Colbert Gives Best Take on YouTube Takedowns*, MEDIASHIFT (Nov. 2, 2006), http://www.pbs.org/mediashift/2006/11/fake-anchor-colbert-gives-best-take-on-youtube-takedowns306/; *see also* Arsham, *supra* note 99, at 778. One option is to supplement the automated system with human review. Helman & Parchomovsky, *supra* note 83, at 1229–34. As for fair and tolerated uses, Helman and Parchomovsky contend that the filtering algorithm might accomplish this by allowing the copyright owner to set a percentage level of allowable use that could be incorporated into the algorithm. *Id.* at 1234.

130. Katyal & Schultz, *supra* note 126, at 88.

131. Arsham, *supra* note 99, at 799–804.

> subordinated via this system to the interests of incumbent ISPs. Both of these concerns may tend to entrench incumbent ISPs, by foreclosing users' challenges to their policies and by producing industry coordination that may create barriers to new entrants to the industry. [132]

In light of the concerns with the previous models, a new model is worth exploring.[133] One such model could supplement (or replace) the DMCA notice and takedown system with a duty-based regime. At the very least, this model would reintroduce preventative measures, restoring the original DMCA balance, and would also address some of the concerns with the above proposals. Before exploring such a model, it is instructive to survey the international community efforts to resolve ISP liability.

V. INTERNATIONAL EFFORTS TO ADDRESS ISP LIABILITY

As ISP liability for online infringement is a global issue, how other countries attempt to solve the issue can shed light on possible domestic solutions. While limited, the following cases and legislation are representative of international efforts to address ISP liability. The efforts in many ways track those of the DMCA and U.S. courts, but also depart from these by broadening ISP liability.

This investigation appropriately begins with the EU, which sets international intellectual property policy through member states' legislation, bilateral trade agreements, and through influence exerted in multilateral intellectual property treaties.[134] The EU efforts begin with the EU Directive

---

132. Mehra & Trimble, *supra* note 92, at 703.

133. One solution would be for courts to interpret the DMCA in light of Congress' intent to avoid "surprising consequences." Kirtsaeng v. John Wiley & Sons, 133 S.Ct. 1351, 1362 (2013); *See, e.g.*, Weinberger v. Hynson, Westcott & Dunning, Inc., 412 U.S. 609, 631–32 (1973) ("It is well established that our task in interpreting separate provisions of a single Act is to give the Act 'the most harmonious, comprehensive meaning possible' in light of the legislative policy and purpose.") (quoting Clark v. Uebersee Finanz-Korporation, A.G., 332 U.S. 480, 488 (1947)). Courts thus have judicial discretion to discern and effect congressional intent when the plain language of the law is not clear. This is unlikely here, particularly as the DMCA is clear as to monitoring duties.

134. *See, e.g.*, GRAEME B. DINWOODIE, WILLIAM O. HENNESSEY, SHIRA PERLMUTTER, AND GRAEME W. AUSTIN, INTERNATIONAL INTELLECTUAL PROPERTY LAW AND POLICY 44 (2d ed. 2008). As one example of the EU's influence on the United States, the EU adopted the EU Term Directive, which extended the copyright term for an additional twenty years to the current term of life of an author plus seventy years. This motivated the United States to pass the Sonny Bono Copyright Term Directive, which similarly extended U.S. copyright terms to life plus seventy years.

concerning the development and growth of the Internet—the E-Commerce Directive[135]—and how that Directive has been interpreted by the Court of Justice of the European Union (CJEU).[136] Like the DMCA, the E-Commerce Directive aims to expedite the development of ISPs without internal barriers; it also aims to further the broader aim of uniting member nations' intellectual property laws.[137]

A. The E-Commerce Directive and Caselaw

Like the DMCA, the E-Commerce Directive provides for a number of safe harbors that protect ISPs from liability when engaging in three types of activities: (1) acting as mere conduits;[138] (2) operating caches (storing information);[139] and (3) hosting information provided by recipients of the service.[140] Other directives and national laws complement the E-Commerce Directive.[141] Most relevant is the Directive on the Enforcement of Intellectual Property Rights ("EU Directive"), which entered into force on May 20, 2004 and creates a general obligation for member states to set up measures and procedures needed to ensure the enforcement of intellectual property rights and to take appropriate action against those responsible for counterfeiting and piracy.[142] The measures are intended to be sufficiently dissuasive without

---

135. Council 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, 2000 O.J. (L 178) 1 (EU) [hereinafter E-Commerce Directive].

136. International treaties such as the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty were the first international efforts to address digital technology. *See* WIPO Copyright Treaty, arts. 11–12, Dec. 20, 1996, S. Treaty Doc. No. 105-17, 36 I.L.M. 65 [hereinafter WCT]; WIPO Performances and Phonograms Treaty, arts. 18–19, Dec. 20, 1996, S. Treaty Doc. No. 105-17, 36 I.L.M 76 [hereinafter WPPT]. The two treaties required member states to, among other things, provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures, and to protect digital rights management information. WCT arts. 11–12; WPPT arts. 18–19. The United States implemented its treaty obligation with the DMCA. *See* Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified in scattered section of 5, 17 and 28 U.S.C.).

137. E-Commerce Directive, *supra* note 135, recital 1. As stated in Recital 1, The Directive seeks to "eliminate barriers that divide the European peoples." *Id.* Importantly, the E-Commerce Directive is not limited to ISP liability; rather, it addresses various e-commerce issues. *Id.*

138. *Id.* art. 12.

139. *Id.* art. 13.

140. *Id.* art. 14. Unlike the DMCA, the E-Commerce Directive does not provide a safe harbor for providing "information location tools." *Cf.* 17 U.S.C. § 512(d) (2014).

141. *See* Council Directive 2004/48/EC, 2004 O.J. (L 157) 45 (EU) [hereinafter EU Directive].

142. The precise relevant language in the EU Directive states: "1. Member States shall provide for the measures, procedures and remedies necessary to ensure the enforcement of the

creating barriers to legitimate trade, and encourage means to safeguard against the abuse of the measures.[143]

During the 1990s, a number of EU Member States began introducing laws that shielded nascent ISPs from liability caused by end users.[144] To avoid inconsistent legal approaches among Member States, in 2000, the EU adopted the E-Commerce Directive. The three relevant provisions of the E-Commerce Directive are Articles 12.1, 12.3, and 15. Article 12.1 provides:

> Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider: (a) does not initiate the transmission; (b) does not select the receiver of the transmission; and (c) does not select or modify the information contained in the transmission.[145]

Article 12.3 provides: "This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement."[146] Finally, Article 15.1 provides that "Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13, and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or

---

intellectual property rights covered by this Directive. Those measures, procedures and remedies shall be fair and equitable and shall not be unnecessarily complicated or costly, or entail unreasonable time-limits or unwarranted delays. 2. Those measures, procedures and remedies shall also be effective, proportionate and dissuasive and shall be applied in such a manner as to avoid the creation of barriers to legitimate trade and to provide for safeguards against their abuse. . The EU Directive is not intended to affect any provisions such as the exceptions contained in Community legislation concerning copyrights and rights related to copyright, nor does it affect the obligations EU countries have under TRIPS. The enumerated purposes of the EU Directive by its drafters are to 1) promote innovation and business competitiveness; 2) safeguard employment in Europe; 3) prevent tax loss and destabilization of markets; 4) ensuring consumer protection; and 5) ensuring the maintenance of public order." *Id.* Ch. 2 § 1 art. 3.

143. *Id.* The E-Commerce Directive is often balanced against the EU Directive.

144. *See, e.g.*, Christina Angelopoulos, *Beyond the Safe Harbours: Harmonising Substantive Intermediary Liability for Copyright Infringement in Europe* 1 (Amsterdam L. Sch., Research Paper No. 2013-72, 2013), http://dare.uva.nl/document/2/136139 ("[A] number of EU Member States started introducing special liability laws in order to shield the budding internet industry from legal uncertainty.").

145. E-Commerce Directive, *supra* note 141, art. 12.1.

146. *Id.* art. 12.3.

circumstances including unlawful activity."[147] These provisions mirror those found in the DMCA.[148]

Because directives instruct member states to attain specific goals but do not specify the means to attain the goals, individual member states must enact implementing domestic legislation, known as "transposition," to give force to the directives.[149] At first glance, individual member state adoption of legislation implementing the E-Commerce Directive suggests that each country has consistent laws regulating ISP liability (particularly with regard to caching, hosting and mere conduit activities). This is not the case. Because transposition leaves member states discretion for implementing laws, states can impose different and additional obligations on ISPs so long as they are consistent with the broad reach of the directives.[150] While each EU member still plays a role in setting the appropriate level of obligation that may be imposed on ISPs to prevent copyright infringement, the Court of Justice of the European Union (CJEU) interprets EU law, including directives; each country is then bound by the CJEU's interpretation.[151] This system prevents the risk that national courts in each EU country will interpret EU law in different ways.[152] In 2010, in a Belgian case, *Scarlet v. SABAM*,[153] the CJEU had its first opportunity to interpret the E-Commerce Directive and the boundaries of ISP liability.

1. Scarlet v. SABAM (CJEU)

In *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*,[154] the CJEU interpreted the E-Commerce Directive as prohibiting member state courts from requiring ISPs (or Internet access providers) from installing a filtering system to prevent copyright

147. *Id.* art. 15.1.

148. As both are intended to implement the WIPO Copyright Treaties, this is no surprise.

149. Article 249 of the Treaty Establishing the European Community (1957 Treaty of Rome, as amended by the 1992 Treaty of Maastricht) provides that "[a] Directive shall be binding as to the result to be achieved . . . but shall leave to the national authorities the choice of form and methods." Treaty Establishing the European Community art. 249 (as in effect 1993) (now Consolidated Version of the Treaty on the Functioning of the European Union art. 288, Oct. 26, 2012 O.J. (C 326) 1 [hereinafter TFEU]).

150. *See id.*

151. TFEU, *supra* note 149, arts. 260–67.

152. National courts are able to seek from the CJEU a "'preliminary ruling," which allows a national court that is in doubt about the interpretation or validity of an EU law to ask the CJEU for advice. *Id.* art. 267.

153. Case C-70/10, 2011 E.C.R. I-11962.

154. *Id.*

infringements. Scarlet was an ISP that only offered access to its users (and no other services, such as downloading or file sharing).[155] SABAM was a management company that represented copyright holders.[156] SABAM concluded that Internet users using Scarlet's services were downloading copyright holders' works, using filesharing software through a peer-to-peer system.[157] A Brussels tribunal ordered Scarlet to block users' sites to prevent the infringement.[158] Scarlet appealed, claiming that, for various technical and practical reasons it was impossible to comply with the order, and that the order was contrary to national law that transposed Article 15 of the E-Commerce Directive prohibiting courts from imposing a general obligation to monitor communications.[159] The Belgian appellate court referred the matter to the CJEU for a preliminary ruling, asking whether an ISP could be required to introduce a filtering system as a preventative measure.[160]

In a landmark ruling the CJEU ruled that courts could not require filtering.[161] After balancing various Directives (including the EU Directive and the E-Commerce Directive), EU law, and national laws, the Court found that the type of filtering Belgium imposed on Scarlet required the ISP to actively monitor all of the data of its customers to prevent future infringement.[162] This, according to the Court, would require the ISP to carry out general monitoring, something which is prohibited by Article 15(1).[163]

Since *Scarlet*, there have been numerous decisions explicating ISP liability; these cases have been consistent with *Scarlet* in not imposing a general monitoring obligation on ISPs. In a similar filtering case, *SABAM v. Netlog*,[164] the CJEU applied the *Scarlet* ruling, which applied to ISPs, to online social networks, ruling that networks did not have an obligation to

155. *Id.* at I-11971.

156. *Id.*

157. *Id.*

158. *Id.*

159. *Id.* at I-11973. Scarlet also claimed that the installation of a filtering system would breach the European Union's law on protection of personal data and secrecy of communication. *Id.* at I-11974.

160. *Id.* at I-11974–75.

161. *Id.* at I-12003–04.

162. *Id.* at I-12001–02.

163. The CJEU also found that the protection of intellectual property rights did not outweigh other rights such as the freedom to conduct a business, guaranteed by the European Charter of Fundamental Rights, Article 16 and the right to protection of personal data and freedom to receive or impart information, which are respectively safeguarded by Articles 8 and 11 of the Charter of Fundamental Right. *Id.* at I-12002.

164. Case C-360/10, 2012 E.C.R. 00000.

implement a general filtering system to prevent the unlawful use of musical and audio-visual work by the users of its network.[165]

Subsequent cases, however, have sought to limit *Scarlet's* reach. For example, in a case that was decided just after *Scarlet*, the British High Court imposed on an ISP an obligation to block access to a website that provided links to pirated copyrighted content. In *Twentieth Century Fox Film Corp v. British Telecommunications Plc.*,[166] Twentieth Century Fox and other movie production companies sought to enjoin British Telecom, UK's largest ISP, from providing its subscribers access to the Newzbin2 Website that provided links to pirated films.[167] The relevant UK copyright law authorized courts to grant an injunction against a service provider where the service provider has actual knowledge of infringement.[168] Here, however, while Twentieth Century Fox had previously successfully sued the operator of the Newzbin site, there was not yet a finding of infringement regarding the Newzbin2 site, which had replaced Newzbin, even though the new site was virtually identical to Newzbin, operating at the same location and in a similar manner.[169] Because Newzbin2 was based offshore and run by unidentified individuals, Twentieth Century argued that it could obtain effective relief only by requiring British Telecom to block access to Newzbin2.[170] Unlike *Scarlet*, here Twentieth Century Fox neither sought general active monitoring nor access to personal data.

British Telecom argued that it had no actual knowledge of infringement and thus had neither an obligation to block nor liability for not blocking. The court found otherwise.[171] Under UK law, implementing the EU Information Society Directive, an ISP could be enjoined if, among other requirements, it had knowledge of infringement.[172] The court held that British Telecom had actual knowledge because it knew that the users and operators of the Newzbin2 Website infringed copyright on a large scale and, in particular, infringed Twentieth Century Fox's copyrights.[173] The court found sufficient that British Telecom had general knowledge of infringement, as opposed to

165. *Id.* at I-11984.

166. Twentieth Century Fox Film Corp. v. British Telecommunications Plc. [2011] EWHC (Ch) 1981, [2012] 1 All ER 806, WL 2747913.

167. *Id.* ¶ 1.

168. *Id.*

169. *Id.* ¶ 2.

170. *Id.* ¶¶ 2–3.

171. *Id.* ¶¶ 120–25.

172. *Id.* ¶ 148.

173. *Id.* ¶ 157.

knowledge of specific instances of infringement.[174] In an arguably broad holding, the court noted that its power extended beyond preventing proven infringement to requiring ISPs to take measures to prevent further, similar infringements.[175] The UK law, according to the court, was to enable a court to issue an injunction against the party best able to bring infringing activities to a halt, in this case British Telecom.[176] Moreover, this purpose was best accomplished by showing a service provider had actual knowledge that subscribers were using its services to infringe, and not by requiring actual knowledge of specific acts of infringement.[177] This type of monitoring and filtering has been referred to as "notice and stay down" (as opposed to notice and takedown), requiring ISPs to prevent anyone from uploading content that has been previously found infringing.

2. *GEMA* (Germany)

Germany, too, has added its own gloss to the CJEU's E-Commerce Directive ruling, as developed in *SABAM*. In *GEMA v. YouTube*,[178] the German High Court held that ISPs could be held to a duty to monitor in certain circumstances. In 2011, GEMA, the German society for musical performing and mechanical reproduction rights, brought an action against YouTube for subscriber infringement because YouTube allegedly had prior notice of hosting infringing content.[179] In April 2012, a Hamburg District Court found that YouTube "made an attributable contribution to the legal infringements" and thus YouTube was liable for subscriber infringements under secondary liability principles.[180] While the court resisted declaring a

174. *Id.*

175. *Id.* ¶ 157.

176. *Id.* ¶¶ 157–58.

177. *Id.* ¶¶ 146–49.

178. LG Hamburg April 20, 2012, 310 O 461/10, https://gmriccio.wordpress.com/2012/04/29/hamburg-district-court-gema-v-youtube-english-translation/.

179. GEMA represents the copyrights of over 64,000 members in Germany and greater than 2 million copyright owners worldwide. Wolfgang Spahr, *GEMA Under Fire From Royalties Dispute With YouTube*, BILLBOARD (June 24, 2011), http://www.billboard.com/biz/articles/news/publishing/1177342/gema-under-fire-for-royalties-dispute-with-youtube.

180. LG Hamburg April 20, 2012, 310 O 461/10, https://gmriccio.wordpress.com/2012/04/29/hamburg-district-court-gema-v-youtube-english-translation/; *Hamburg District Court—GEMA v. YouTube (English Translation)*, COPYRIGHT & INTERNET (Apr. 29, 2012), http://gmriccio.wordpress.com/2012/04/29/hamburg-district-court-gema-v-youtube-english-translation/.

general obligation to monitor, it did sanction more limited monitoring, stating:

> [I]t is in principle not expected that the operator of an internet trading platform will examine every offer for possible legal contravention prior to publication on the Internet. However, if a clear legal contravention is pointed out to him, he must not only block the specific offer without delay, he must also take precautions to ensure that further such legal contraventions do not occur where possible."[181]

YouTube, relying on *SABAM v. Netlog*, claimed that it had no monitoring responsibility. The court dismissed this contention. Unlike *Netlog* (and *Scarlet*), the court noted that GEMA was not seeking preventative monitoring of all video clips uploaded onto YouTube, but was instead seeking monitoring and filtering of specific disputed music titles, of which YouTube had notice, i.e., a "notice and stay down" monitoring scheme.[182]

In *GEMA v. RapidShare*,[183] Germany's Federal Court of Justice again held against ISPs, holding that the Swiss file-hosting service RapidShare has an obligation to monitor outside sites that link to its services to ensure that links do not provide users access to illegal material.[184] GEMA alleged that 4,800 copyrighted files were illegally shared via the RapidShare site and that RapidShare should be held liable. The Court found that a number of RapidShare's actions contributed to infringement, including: (1) RapidShare's revenues were generated through premium accounts that enhanced massive data downloads; (2) RapidShare's service provided incentives for third parties to illegally share copyrighted content; and (3) RapidShare's users had anonymous accounts.[185] The Court thus found it appropriate to impose additional duties on RapidShare, namely requiring that it not only delete files containing copyrighted material as soon as it was

---

181. LG Hamburg April 20, 2012, 310 O 461/10, https://gmriccio.wordpress.com/2012/04/29/hamburg-district-court-gema-v-youtube-english-translation/ (citing *cf.* Bundesgerichtshof [BGH] [Federal Court of Justice] 2011, Gewerblicher Rechtsschutz und Urheberrecht [GRUR] 21 (26), 2011 (Ger.)).

182. *Id.*

183. Bundesgerichtshof [BGH] [Federal Court of Justice] Aug. 16, 2013, Gewerblicher Rechtsschutz und Urheberrecht [GRUR] 1030, 2013 (Ger.).

184. Tom Pakinkis, *GEMA Hails 'Landmark' Court Ruling Against RapidShare in Germany*, MUSICWEEK (Aug. 19, 2013), http://www.musicweek.com/news/read/gema-hails-landmark-court-ruling-against-rapidshare-in-germany/055779.

185. Alexander Harguth, *File Hosting in Germany Carries Increased Copyright Policing Duties***,** MCDERMOTT WILL & EMERY: IP UPDATE, Oct. 2013, at 10, 10–11, http://www.mwe.com/files/Uploads/Documents/News/IP%20Update_October%202013.pdf.

notified by a rights holder, but also that it take steps to prevent similar infringements by other users in the future.[186]

Moreover, the Court required RapidShare to actively monitor incoming links on *other sites* to discover if they, too, allow users access to copyrighted files.[187] RapidShare must do so as soon as it receives a specific reason to do so (e.g., a notice from the copyright holder), and must ensure that those files become inaccessible to the public.[188] RapidShare should use "technically and economically reasonable measures," and "all possible resources such as search engines, Facebook, Twitter or web crawlers to identify such links that were rendered publicly accessible by the users through link lists."[189]

These cases evince EU member countries' struggle to stay within the bounds of the E-Commerce Directive by not imposing a *general monitoring* duty, while also expanding ISP liability short of this boundary to ensure effective enforcement of intellectual property rights. The struggle to find a balance in requiring ISPs to play a more active role in curbing infringement is also seen in various countries' legislation. France and England have led such efforts.

---

186. *Id.* at 11.

187. *Id.*

188. *Id.*

189. *Id.* at 10–11. In Switzerland, courts have refused to impose additional obligations on ISPs to monitor accounts or to require notice and stay down procedures. In *BREIN v. Ziggo*, the anti-piracy group BREIN (on behalf of copyright holders) sued Ziggo (the Netherlands' largest ISP) as well as a rival ISP XS4ALL, attempting to force Ziggo to block access to the website "The Pirate Bay," a torrent site that is arguably the most censored site on the Internet. *Stichting Bescherming Rechten Entm't Industrie Nederland (BREIN) v. Ziggo BV*, (District Court of the Hague, 19 July 2010). BREIN won their case below. *Id.* at § 2.4. On appeal, the Court of The Hague ruled in favor of Ziggo, holding that the imposed blockade was disproportionate, ineffective, and a hindrance to Internet providers' entrepreneurial freedoms. *Id.* at § 4. Even if Ziggo was required to block access, piracy was not thwarted, as users simply circumvented the block or found other ways to access Pirate Bay and torrent copyrighted works from other sites. *Id.* The Court balanced intellectual property rights with ISPs' entrepreneurial freedom, which is found in the Charter of Fundamental Rights of the European Union, and found that the balance tipped in favor of ISPs' rights. *Id.* at § 5. "The circumstance that, despite the blockade, the number of illegal downloaders has increased indicates that newcomers, at least a significant number of them, are not deterred by a blockade to start downloading from illegal sources." Loek Essers, *Dutch court ends Pirate Bay blockcade after digital piracy continued to thrive*, PCWORLD (Jan. 28, 2014), http://www.pcworld.com/article/2092040/dutch-court-finds-pirate-bay-block-ineffective-ends-it.html. *But see* DMCA § 512(d) (no liability for "referring or linking users to an online location containing infringing material or infringing activity").

B. Legislative Responses

1. Frances's HADOPI

In 2009, France adopted the controversial HADOPI law, ushering in the first graduated response system. [190] HADOPI, a government agency, ran under a mandatory, statutory regime that requires ISPs to terminate users' services for repeat offenses (three).[191] The law allowed courts to order ISPs to "take any measure appropriate to prevent or stop online copyright infringement."[192] When HADOPI initiated the graduated response procedure, the ISPs were required to disclose to HADOPI subscriber information within eight days after receiving the request. To protect subscriber privacy, the law provided that only HADOPI administrative agents could access the personal data, which was to be deleted two months after it was disclosed if no further action is taken.[193]

---

190. Nate Anderson, *France Passes Harsh Anti-P2P Three-Strikes Law (Again)*, ARS TECHNICA (Sept. 15, 2009), http://arstechnica.com/tech-policy/2009/09/france-passes-harsh-anti-p2p-three-strikes-law-again/. The DMCA does require ISPs to institute a "repeat offender" procedure, but does not set forth specific requirements for this procedure, stating: "a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers." DMCA § 512(i)(1)(A).

191. Alain Strowel, *Internet Piracy as a Wake-Up Call for Copyright Law Makers—Is the "Graduated Response" a Good Reply?*, 1 W.I.P.O.J. 75, 80 (2009). *See also* Ross Drath, Comment, *Hotfile, Megaupload, and the Future of Copyright on the Internet: What Can Cyberlockers Tell Us About DMCA Reform?*, 12 J. MARSHALL REV. INTELL. PROP. L. 204, 234 (2012). The article describes the United States' attempt to create a similar gradual response system, albeit with limited government involvement. *Id.* ("Faced with high costs and uncertain outcomes when litigating against service providers, a public relations nightmare when litigating against users, and an inability to secure legislative amendments to the DMCA, the content industry has shifted in recent years to a strategy termed 'graduated response.' This approach focuses on education, with the goal of inducing casual users of pirated content to seek out legal alternatives. In July of 2011, a large consortium of major copyright owners (including the MPAA, the RIAA, and their members) teamed up with a group of major service providers (including Comcast, TimeWarner Cable, Verizon, AT&T, and Cablevision) to create the Center for Copyright Information ('CCI'), which will administer the newly created 'Copyright Alert System' ('CAS'). The system requires ISPs to send up to six notices to users accused of infringement by copyright owners. Though implementation of the CAS has been delayed, CCI's Executive Director recently confirmed that the system would be online in the near future." (Internal citations omitted)).

192. *France*, GLOBAL CENSORSHIP CHOKEPOINTS, https://globalchokepoints.org/countries/france (last visited Sept. 25, 2015).

193. In addition, the data is deleted fourteen months after the first warning, twenty-one months after a second warning, and removed from HADOPI's database one year after the public prosecutor files an infringement charge. *See* Décret n° 2010-236 du 5 mars 2010 relatif au traitement automatisé de données à caractère personnel autorisé par l'article L. 331-29 du code

Almost immediately, France's HADOPI law drew criticism.[194] Some claimed that the law was inconsistent with principles of due process, innovation, and free expression.[195] During its brief stint, HADOPI sent one million warning emails, 99,000 "strike two" letters, and identified 314 people for referral to the courts for possible disconnection.[196] In the end, however, HADOPI only ended up disconnecting a single French broadband ISP customer for copyright infringement**.**[197]

Citing extraordinary costs and scant results, France ended the program, opting instead to adopt an automatic fine system.[198] France's culture minister, Aurelie Filippetti, quipped: "€12 million per year and 60 officials; that's an expensive way to send 1 million emails."[199] Filippetti also complained that "the suspension of Internet access seems to be a disproportionate penalty given the intended goal."[200]

2. England's Digital Economy Act

HADOPI's failure did not dissuade similar attempts. In 2009, to implement "Digital Britain"—the United Kingdom's strategy to bring its economy into the digital era—the House of Lords introduced the Digital Economy Act (DEA). The DEA's copyright provisions included both measures intended to help users, such as digital rights management provisions allowing users to easily identify and better negotiate with rights holders, and also measures intended to assist rights holders in enforcing their

---

de la propriété intellectuelle dénommé « Système de gestion des mesures pour la protection des œuvres sur internet» [Decree No. 2010-236 of March 5, 2010 relating to the automated processing of personal data authorized by Article L. 331-29 of the Code of Intellectual Property referred to as "measurement management system for the protection of works on the Internet"], 56 Journal Officiel de la Republique Francaise [J.O.] [Official Gazette of France], March 7, 2010, p. 4680.

194. *See France*, *supra* note 191.

195. Gwen Hinze, *Preliminary Analysis of the Officially Release ACTA Text*, ELEC. FRONTIER FOUND. (Apr. 22, 2010), https://www.eff.org/deeplinks/2010/04/eff-analysis-officially-released-acta-text.

196. Rainey Reitman, *Repealing French Three Strikes Law is the Next Step to Safeguarding Free Expression*, ELEC. FRONTIER FOUND. (Aug. 8, 2012), https://www.eff.org/deeplinks/2012/08/repeal-french-three-strikes-law.

197. Mark Jackson, *France Replaces ISP Cut-Off Policy for Internet Piracy with Automatic Fines*, ISPREVIEW (July 10, 2013), http://www.ispreview.co.uk/index.php/2013/07/france-replaces-isp-cut-off-policy-for-internet-piracy-with-fines.html.

198. *Id.*

199. Reitman, *supra* note 196.

200. *Id.*

intellectual property rights.[201] The enforcement measures required ISPs to prevent infringing activity before it occurred. Unlike the conduct at issue in *Scarlet*, however, Section 17 of the DEA granted the Secretary of State power to make regulations enabling courts to require ISPs to block certain sites that are *proven* infringement sites.[202] The DEA also has a graduated response element.

As with HADOPI, here, too, the DEA enforcement provisions were controversial. Civil liberties and consumer rights advocates criticized the provisions as violating basic fundamental rights such as data protection, privacy, and freedom of expression, and further cautioned that the DEA provisions constituted censorship and failed to provide for court hearings before imposing sanctions.[203] Rather than impose such contentious and divisive measures, these groups argued that online copyright infringement should instead be addressed by making copyrighted content more affordable and in a variety of user-friendly formats.[204]

Amidst such opposition, the government placed the DEA enforcement provisions on hold, while moving forward with other DEA provisions.[205] The

---

201. The Government's official position is reflected in this statement: "We want a framework for copyright and performers' rights that reflects the needs of the digital age, and gives the UK's creative industries the chance to develop new legitimate digital products delivered in the way people want, at a price that is fair. That means we need to make doing business easier in this area, and to significantly reduce the amount of online infringement of copyright." Anne Barron, *'Graduated Response' à l'Anglaise: Online Copyright Infringement and the Digital Economy Act 2010*, 3(2) JOURNAL OF MEDIA LAW 305, 307 (2011), http://dx.doi.org/10.5235/175776311799280773 (citing BIS/DCMS, "Copyright: Factsheet" (Nov. 2009)).

202. *Id.* at 308.

203. Spain has recently passed legislation increasing copyright holders' rights vis a vis ISPs. Under the Sinde-Wert law, which went into effect on March 1, 2012, an Intellectual Property Commission has the authority to close down websites that link to content infringing IP rights, and allow copyright holders to seek the identity of potential infringers. As the key targets of the Sinde-Wert law are owners of websites that offer lists of links leading directly to copyrighted works, end users, "neutral" search engines and P2P programs that allow sharing of content are all exempt from punishment. *Anti-piracy Sinde-Wert Law Becomes Obsolete on First Month of Life*, EITB (Mar. 26, 2012), http://www.eitb.eus/en/news/technology/detail/857392/antipiracy--sindewert-law-becomes-obsolete-first-month-life/.

204. *Id.*

205. Some of the unresolved questions concerned the balance of intellectual property rights with other EU rights, including freedom of expression, privacy, data protection and the interception of Communications. *See* Barron, *supra* note 178, at 309. Australia is also considering a graduated response system. *See* Murray Griffin, *Australian AG Unswayed by Fair Use Recommendation but Sees Merits in New Controls on ISPs*, INTELL. PROP. L. RESOURCE CTR. (Feb. 18, 2014), http://iplaw.bna.com/iprc/display/alpha_hash.adp?mode=si&frag_id=41841374&item=561&prod=wiln&cat=INDUSTRY.

Government's Department for Culture, Media & Sports stated that it expects broadband ISPs to start issuing their first notification letters to suspected infringers towards the end of 2015, rather than the initial 2014 date.[206] Much of the delay is a result of continued evaluation of costs (i.e., how the costs of the measures are to be shared between ISPs and copyright holders), the legal viability and practicality of the measures, and political disagreements.[207]

Other countries such as South Korea, Spain, Italy, and Australia have either passed similar graduated response laws or are contemplating such laws.[208]

C. Non-copyright cases: ISP Liability for Defamatory Content

1. Estonia

Other, non-copyright cases and criminal copyright cases might shed light on the appropriate balance between ISPs' rights and copyright enforcement.[209] In Estonia, the Estonia High Court in *Delfi AS v. Estonia*,[210] held that an ISP was liable for defamatory content posted by the site's users.[211] The Court ruled that a safe harbor provision did not protect the ISP because the ISP was more than a passive site.[212] Delfi AS, a company that owns and operates one of the largest Internet news sites in Estonia, published an article criticizing a ferry transport company, alleging that the company destroyed public ice roads in order to keep Estonian citizens dependent on the company's ferry service.[213] Delfi permits users to publish anonymous comments on the articles it publishes.[214] The ferry transport article attracted

206. Mark Jackson, *UPD Internet Piracy Warning Letters from UK ISPs Delayed to Late 2015*, ISPREVIEW (June 5, 2013), http://www.ispreview.co.uk/index.php/2013/06/first-internet-piracy-warning-letters-from-uk-isps-delayed-until-late-2015.html.

207. *Id.*

208. *See, e.g.*, *South Korea*, GLOBAL CENSORSHIP CHOKEPOINTS, https://globalchokepoints.org/countries/south-korea (last visited Nov. 12, 2015) (South Korea suspended its law in 2010).

209. Rulings regarding, for example, ISP liability for posting defamatory content might be appropriately applied to posting of infringing copyrighted content. *See, e.g.*, Robins, *supra* note 30, at 22–23 ("It [] seem[s] disingenuous for an intermediary to claim it can only identify one type of inappropriate content.").

210. EUR. CT. H.R. (Oct. 10, 2013), http://hudoc.echr.coe.int/eng?i=001-126635.

211. *Id.* ¶ 29.

212. *See id.* ¶¶ 25, 27.

213. *Id.* ¶ 12.

214. *Id.* ¶ 8.

185 comments, twenty of which contained personal threats and offensive language directed toward the company's sole/majority shareholder and member of its supervisory board.[215] The company's lawyers asked Delfi to remove the offensive comments and requested compensatory damages.[216] Delfi removed the comments that same day, but refused to compensate the company for damages, claiming that its only obligation was to remove offensive content under Estonia's notice and takedown provision (this provision tracked the obligations under the E-Commerce Directive).[217]

The Supreme Court of Estonia affirmed the appeal court's holding that Delfi was a co-publisher, ineligible for the safe harbor protection.[218] Delfi had a legal obligation to avoid causing damage to other persons (Estonian Law of Obligations) and should have prevented clearly unlawful comments from being published.[219] The Court found it significant that after the comments had been published, Delfi failed to remove them "*on its own initiative*."[220]

Delfi then filed a complaint against the Supreme Court of Estonia before the European Court of Human Rights (ECtHR) claiming that its right to freedom of expression was violated.[221] The Court ruled that the Estonian Supreme Court's decision to impose broad liability on Delfi was a proportionate and justified interference with Delfi's freedom of expression.[222] The ECtHR noted that the article addressed a topic of public interest, but the article negatively affected a large number of people, and Delfi should have realized that publishing the article would cause negative reactions against the company and its managers.[223] Considering the reputation of comments on Delfi's site, there was a "higher-than-average risk that the negative comments posted on the article would go beyond the boundaries of acceptable criticism and reach the level of gratuitous insult or hate speech."[224] Also, the number of comments posted on the article was higher than usual, and thus Delfi should have exercised a degree of caution in order to avoid being held liable for an infringement of another person's

215. *Id.* ¶ 13.
216. *Id.* ¶ 14.
217. *Id.* ¶¶ 15–16.
218. *Id.* ¶ 28.
219. *Id.* ¶ 29.
220. *Id.* (emphasis added).
221. *Id.* ¶¶ 1–3.
222. *Id.* ¶ 94.
223. *Id.* ¶ 86.
224. *Id.*

reputation.[225] Additionally, Delfi had a monitoring and filtering system, a notice and takedown mechanism, and had at other times prevented offensive comments from being posted.[226] Delfi had a disclaimer in place stating that writers of the comments were responsible for their comments, and not the company itself.[227] Its filter automatically deleted comments containing certain vulgar words, and Delfi administrators occasionally removed comments on their own initiative.[228] While Delfi did not entirely neglect its duty to avoid causing harm to others' reputations, the filtering system was easily circumvented.[229] Also, while Delfi prevented some of the offensive comments, it failed to do so for a number of others.[230] The Court thus found that the filtering system was insufficient for preventing harm caused to third parties.[231]

Finally, the Court noted that the filter and notice and takedown measures, as a whole, did not ensure sufficient protection of the rights of third parties.[232] News articles, attracting readers, and attracting user comments were all part of Delfi's business activities.[233] This was relevant in determining the proportionality of the inference with Delfi's freedom of expression.[234] Delfi was in a better position than the ferry company (or other third parties) to know about an article to be published, to predict the nature of the comments that the article would receive, and to take technical or manual measures to prevent defamatory statements from being made public.[235] Because Delfi exercised a substantial degree of control over the comments published on its portal, even if it did not make full use of the capabilities of that control, liability for posting of the defamatory content outweighed Delfi's freedom of expression.[236]

---

225. *Id.*
226. *Id.* ¶ 87.
227. *Id.*
228. *Id.*
229. *Id.*
230. *Id.*
231. *Id.*
232. *Id.* ¶ 89.
233. *Id.*
234. *Id.*
235. *Id.* This should resonate with those who claim that ISPs are in a better position than copyright holders to detect infringement.
236. *Id.* ¶¶ 89, 94.

2. Switzerland

In a similar case in Switzerland, the Swiss Federal Supreme Court held that an ISP can be liable for defamatory content posted by its users.[237] The appellant was a Swiss publishing house and editor of a daily newspaper. Its website contained an abbreviated version of the newspaper and links to its readers' blogs, which the publishing house also hosted.[238] The respondent was a Geneva municipality mayor and a member of a foundation that was created to aid the Cantonal Bank of Geneva with its financial troubles. The mayor was personally attacked on a blog and his financial operations at the foundation and bank were questioned. The mayor requested that the court issue interim measures requiring the blogger and ISP to remove the blog post and prevent it from publishing the post in the future. He then instituted full proceedings against both parties claiming that his right to personality had been infringed.[239] The ISP was found liable and appealed to the Federal Supreme Court claiming it could not be held liable for content generated and published by its readers on blogs.[240]

The Federal Supreme Court acknowledged that Switzerland had no specific legal provisions dealing with ISP liability, and applied the Swiss Civil Code provisions. Under the Civil Code, another could be held liable if it contributed to illegal conduct. The Court thus had to resolve whether the mere hosting of a blog was a "contribution."[241] The Court held that it was. The Court analogized a blog host to that of a printed journal that publishes readers' letters and concluded that the ISP, which provided the required technical infrastructure to create and make available user-generated content, contributed to the infringement and was, therefore, liable. Further, since no fault is required for liability, the Court held that the ISP did not have to be aware of the infringement or have knowledge of the published content. Interestingly, the Court made a plea to the legislature to consider whether protective measures should be implemented for ISPs in this situation.

D. Criminal Copyright Infringement—Argentina

In addition to the non-copyright cases, criminal copyright cases against ISPs also may be informative in gleaning trends in the international response

237. Eva-Maria Strobel, *Internet Service Providers Run Liability Gauntlet in Switzerland*, WORLD INTELL. PROP. REP., Oct. 2013, at 43, 44.

238. *Id.* at 43.

239. *Id.* at 44.

240. *Id.*

241. *Id.*

to ISP liability. In Argentina, for example, in 2011 la Cámara Argentina de Libro (CAL), Argentina's Book Chamber, filed a complaint against the operators of Argentina's most popular social networking Web site Taringa!.[242] The National Chamber of Criminal Appeals in Argentina confirmed the lower court's decision to hold the three operators of Taringa!, Alberto Nakayama, Matias Botbol and Herman Botbol, criminally liable under Argentina's Intellectual Property Law 11.723 for offenses committed by their users.[243] The owners were collectively found guilty of assisting copyright infringement; Taringa! was found responsible for sending in excess of 72 million visitors to Megaupload, a haven for illegal, downloadable copies of music and movies, over a thirteen month period.[244]

Rather than further appealing to the highest court, the operators of Taringa! settled with CAL out of court. The agreement resulted in promises by Taringa! to implement a tool on its social network that would disable any found links to the Megaupload site which were deemed harmful to copyright owners' rights. This led to Taringa! operating a Notice and Takedown system based on the DMCA.[245] In addition to having the criminal charges against Taringa!'s operators removed, CAL agreed to release for publication on the Internet any works whose authors did not require access fee payment; and also publish the books of small publishers and authors for whom the Internet is a means of broadcasting and advertisement.[246] In April 2013 Taringa!'s operators and several intellectual property organizations agreed to a joint effort to make more accessible cultural commodities online, while staying within the bounds of the law, opening up further dialogue and the possibility of lobbying to broaden ISP protection in Argentina.[247]

---

242. Franco Varise, *El sitio Taringa! superó una dura prueba judicial*, LANACÍON.COM (Mar. 27, 2012), http://www.lanacion.com.ar/1459934-el-sitio-taringa-supero-una-dura-prueba-judicial.

243. Regimen Legal De La Propiedad Intelectual, Ley 11.723, 30-09-33 (Arg.), *translated in* LEGAL INTELLECTUAL PROP. REGIME (World Intellectual Prop. Org., 2011) http://www.wipo.int/wipolex/en/text.jsp?file_id=225488.

244. Varise, *supra* note 242. The Botbol brothers were also prosecuted under Article 72 of Law 11.723. "Any person publishing, selling, or reproducing by any means or instrument an unpublished or published work without authorization from its author or his legal successors" shall be punished with the penalty established by Article 172 of the Penal Code (one month to six years imprisonment). *Supra* note 243.

245. *Taringa! introdujo mejoras en el sistema de denuncias por derecho de autor*, TÉLAM TECNOLOGÍA (Dec. 11, 2012, 2:03 PM), http://www.telam.com.ar/notas/201212/911-taringa-introdujo-mejoras-en-el-sistema-de-denuncias-por-derecho-de-autor.html.

246. *Id.*

247. *Taringa y las entidades de protección intelectual firmaron un acuerdo de trabajo conjunto*, TÉLAM TECNOLOGÍA (Apr. 12, 2013, 3:45 PM),

While this section is necessarily limited and not an exhaustive review of international responses, it is nevertheless representative of such responses. Arguably, an international trend can be discerned from this review. While countries are constrained from imposing a general obligation on ISPs to ex ante monitor and filter for infringing content, countries are willing to expand liability by requiring ISP monitoring for infringing content of which the ISP was previously aware.[248] Beyond this, the jury is still out on whether ISPs should have additional obligations, such as limiting users' rights under some form of a graduated response system. In short, while countries appear willing to impose additional duties on ISPs, the extent of those additional duties is unclear.

VI. A DUTY-BASED APPROACH TO ISP LIABILITY

In determining the appropriate level of ISP liability, a new regime, DMCA 2.0, is proposed here. The regime would require that ISPs use reasonable measures to prevent infringement in addition to the ex post duties to remove infringing material after receiving notice. To flesh out an appropriate standard, two other areas help inform that standard. The first is an area from which copyright law has previously sought guidance, namely, employment law.[249] The second is a pre-Internet era context in which copyright holders and those in a position to detect and deter infringement cooperated to prevent and redress infringement.

---

http://www.telam.com.ar/notas/201304/13860-taringa-y-las-entidades-de-proteccion-intelectual-firmaron-un-acuerdo-de-trabajo-conjunto.html.

248. This is similar to allegations in *Viacom* regarding red flag knowledge. *See* Viacom Int'l, Inc. v. YouTube, Inc., 718 F. Supp. 2d 514, 520–21 (2010).

249. The claim here is not that employers and ISPs are the same. Surely, they are not. Employers have a closer tie to their employees, justifying certain duties, and have less of a burden in supervising their employees than an ISP would in supervising its subscribers. In addition, the social harms associated with sexual harassment and employee misconduct are greater than the social harms attending copyright infringement. In the employment context free speech and prior restraint concerns are also less present. Nevertheless, the *underlying principles* from employment law can provide guidance, as they did for contributory and vicarious liability. Moreover, as employers are able to exercise some control over their employees, and gain substantial benefits from their employees, so, too, are ISPs able to exercise some level of control and reap certain benefits from their subscribers; this might suggest reliance on employment law principles is not entirely inappropriate.

A. Reintroducing Preventative Measures—Sexual Harassment Structure

As seen above, employment law's sexual harassment framework contains both strict liability for supervisory adverse employment actions and duty-based liability for other supervisory misconduct. This approach has appeal. When a plaintiff-employee asserts a sexual harassment claim under Title VII, the *Ellerth/Faragher* affirmative defense is available to employers who demonstrate that they took reasonable measures to prevent harassment. To satisfy this obligation, employers commonly adopt sexual harassment policies. The employer must demonstrate that these policies are both widely distributed to its employers and that the policies are effective.[250] The first requirement is easily met. The second, effectiveness, is trickier.

In *Barrett v. Applied Radiant Energy Corporation*,[251] the Fourth Circuit affirmed the district court's finding that the employer exercised reasonable preventative care and that the plaintiff-employee unreasonably failed to take advantage of an effective corporate sexual harassment policy.[252] The written policy clearly stated that harassment based on race, color, sex, marital status, etc., is not tolerated and that any form of harassment is a violation.[253] It defined sexual harassment as "sexual advances, requests for sexual favors, unwelcome or offensive touching and other verbal, graphic or physical conduct of a sexual nature," and also prohibited the posting of offensive materials.[254] The policy also contained a bypass clause allowing employees to talk to "higher ups" whenever necessary in order to avoid uncomfortable or futile situations. The bypass clause stated:

> If you do not feel that the matter can be discussed with your supervisor, you should contact any member of the management team, male or female, with whom you feel comfortable discussing

250. *See* Hetreed v. Allstate Ins. Co., No. 96 C 2021, 1999 WL 311728, at *5 (N.D. Ill. May 12, 1999) *aff'd*, 6 F. App'x 397 (7th Cir. 2001) ("While the mere existence of a policy is not enough to establish adequate preventive action, there is no evidence in the record to indicate that this one was ineffective.").

251. 240 F.3d 262 (4th Cir. 2001).

252. *Id.* at 264. At least one court held that a jury could find the mere existence of a verbal sexual harassment policy can satisfy the first prong of the *Ellerth/Faragher* affirmative defense. *See* Turner v. Saloon, Ltd., 715 F. Supp. 2d 830, 836 (N.D. Ill. 2010) ("Although it is undisputed that [employer] had no written sexual harassment policy, such a policy is not necessary in every instance as a matter of law to satisfy the first prong of the *Ellerth/Faragher* defense. . . . Further, finding that [employer] was unreasonable as a matter of law is inappropriate because the record indicates that [employer] had a verbal sexual harassment policy."). This case seems an outlier.

253. *Barrett*, 240 F.3d at 265.

254. *Id.*

> the situation including the President. You may be assured that your complaint will be dealt with immediately and will be kept as confidential as possible. You will not be penalized in any way for reporting a harassment problem.[255]

Although the mere existence of a policy is not enough on its own to prove reasonable preventative action,[256] the inclusion of the bypass clause was enough for the court to accept the effectiveness of the policy.[257] Because the policy was universally distributed among and signed by employees, the court shifted the burden of proof to the employee to prove that the "employer adopted or administered an anti-harassment policy in bad faith or that the policy was otherwise defective or dysfunctional."[258] The employee could not meet this burden and the court ultimately held that the policy was effective.[259]

In *Adams v. O'Reilly Automotive, Inc.*,[260] the Eighth Circuit took a more expansive approach. While the court analyzed the content of the policy,[261] it also looked to actual implementation to determine effectiveness.[262] A policy may be ineffective not only if it is "unreasonable," but also if it is unenforced.[263] Here, the plaintiff-employee claimed that at least four of her colleagues were harassed and followed proper complaint protocol, but the employer ignored the complaints, rendering the policy ineffective.[264] The employer countered with evidence of past enforcement.[265] Ultimately, the court found "that a reasonable jury could not conclude on this record that [the

---

255. *Id.*

256. *See* Weger v. City of Ladue, 500 F.3d 710, 719 (8th Cir. 2007) ("Though the [employer's] distribution of a valid antiharassment policy provides 'compelling proof that [it] exercised reasonable care in preventing and promptly correcting sexual harassment,' . . . it is not dispositive." (quoting *Barrett*, 240 F.3d at 266). *But see* Chapman v. Carmike Cinemas, 307 F. App'x 164, 169 (10th Cir. 2009) ("We conclude that because [employer] showed that it promulgated, disseminated, and conducted training on an anti-harassment policy, it established the first element of the defense.").

257. *Barrett*, 240 F.3d at 265; *see also* Shaw v. AutoZone, Inc., 180 F.3d 806, 812 (7th Cir. 1999) (holding that distributed policies that encourage contacting management satisfy the ex-ante prong of the affirmative defense).

258. *Id.* at 266 (quoting Brown v. Perry, 184 F.3d 388, 396 (4th Cir. 1999)).

259. *Barrett*, 240 F.3d at 264.

260. 538 F.3d 926 (8th Cir. 2008).

261. *Id.* at 929.

262. *Id.* at 931.

263. *Id*. ("If the policy was unreasonable or unenforced then it cannot be used to demonstrate that O'Reilly exercised reasonable care in preventing and correcting sexual harassment.").

264. *Id.* at 930–31.

265. *Id.* at 931.

employer] did not implement its stated anti-harassment policy in an effective way."[266]

In *Leoughman v. Malnati Org., Inc.*,[267] the Seventh Circuit found that a policy was ineffective because it failed to halt ongoing harassment.[268] There, the plaintiff-employee, who was harassed multiple times by multiple people, followed the instructions set out in the employee manual and informed management of the harassment.[269] According to the appellate court, "the consistent stream of harassment at the restaurant suggests that [the employer's] policy was actually not very effective at all."[270]

Similarly, in *Gentry v. Export Packaging, Co.*,[271] the Seventh Circuit stated that "the mere creation of a sexual harassment policy will not shield a company from its responsibility to actively prevent sexual harassment in the workplace." The court required that the policy "provide for a meaningful process whereby an employee can express his or her concerns regarding an individual within a working environment," and whether the employer "took reasonable care to prevent sexual harassment."[272] The *Gentry* court found that the policy "raise[d] concerns" because even though it advised employees to report sexual harassment to a Human Resources Representative, management did not post whom they considered to be a Human Resources Representative, and no consensus existed within the management regarding who assumed the position of Human Resources Representative.[273]

---

266. *Adams*, 538 F.3d at 931.

267. 395 F.3d 404 (7th Cir. 2005).

268. *Loughman*, 395 F.3d at 408; *see also* Spriggs v. Diamond Auto Glass, 242 F.3d 179, 188 (4th Cir. 2001) ("Under these circumstances, a jury could rationally conclude that, although [employer's] institution of an anti-harassment policy represented a reasonable step toward preventing the type of abuse suffered by [employee-plaintiff], the company unreasonably failed to correct [supervisor's] offending behavior by neglecting to enforce the policy. [Employer's] entitlement to the affirmative defense is therefore a triable issue.").

269. Loughman v. Malnati Org., Inc., No. 02 C 7899, 2004 WL 524444, at *1 (N.D. Ill. Jan. 30, 2004) *rev'd and remanded*, *Loughman*, 395 F.3d 404 ("Under [employer's] policy an employee has the option of reporting harassment to the corporate office via a telephone number provided in the handbook, or directly to any of three female managers.").

270. *Loughman*, 395 F.3d at 407. The court remanded the case for a jury to determine the effectiveness of the policy. *Id.* at 408.

271. 238 F.3d 842 (7th Cir. 2001).

272. *Id.* at 847 ("[T]he law does not require success—it only requires that an employer act reasonably to prevent sexual harassment." (quoting Shaw v. AutoZone, Inc., 180 F.3d 806, 812 (7th Cir. 1999))).

273. *Id.* at 847–48.

B. Copyright Holder Cooperation—Customs and Border Patrol Structure

In 1993, in the pre-Internet era, Congress enacted the North American Free Trade Agreement Implementation Act (also known as the Customs Modification or "Mod" Act),[274] which outlines the copyright protections implemented by the United States Customs and Border Patrol ("CBP"). The Act, in part, was designed to bring copyright holders and the CBP together to prevent the importation of materials that infringe both copyrights and trademark rights.[275] Through the Mod Act, the CBP is vested with authority to detain and seize "piratical copies" of copyrighted works. The Act defines "piratical copies" as being "actual or substantially similar copies of a registered copyrighted work, produced and imported in contravention of the rights of the copyright owner." The CBP focuses its enforcement only on those copyrights that have been registered with its agency.[276] In order for the CBP to determine if imports are "piratical copies" of copyrighted works, it must have a copy of the work on file. The initial onus is on the copyright owner to record the work with the CBP.[277] The owner registers with the CBP after obtaining copyright registration from the United States Copyright Office.[278] The owner must provide the CBP with the U.S. Copyright Office registration number, the title of the copyrighted work, a description of the copyrighted work, any foreign title of the work, and other clerical information of the copyright owner.[279]

The authority of the CBP differs depending on the type of piratical work it encounters. For a "clearly piratical work" (defined as having an "overwhelming and substantial similarity between the copyrighted elements of the protected work and the suspect item so as to clearly indicate that one work is based upon the other"), the infringing articles are subject to seizure

---

274. North American Free Trade Agreement Implementation Act, Pub. L. No. 103-182, 107 Stat. 2057.

275. U.S. CUSTOMS & BORDER PROTECTION, WHAT EVERY MEMBER OF THE TRADE COMMUNITY SHOULD KNOW ABOUT: CBP ENFORCEMENT OF INTELLECTUAL PROPERTY RIGHTS 6 (2012).

276. *Id.*

277. U.S. Customs & Border Prot. Directive 2310-005B, Copyright Protection (2001), http://www.cbp.gov/sites/default/files/documents/copyright_pro_3.pdf [hereinafter CBP Directive].

278. U.S. CUSTOMS & BORDER PROT., WHAT EVERY MEMBER OF THE TRADE COMMUNITY SHOULD KNOW ABOUT: CBP ENFORCEMENT OF INTELLECTUAL PROPERTY RIGHTS 14 (2012).

279. *See id.* (citing 19 C.F.R § 133.31–37 (2007)).

and forfeiture.[280] Customs will notify the importer that her goods have been deemed subject to seizure or forfeiture for being introduced (or for the attempted introduction) into the United States contrary to law.[281] The importer then has 30 days in which to reply to the notification, stating all facts that the importer believes warrants relief from forfeiture.[282]

If the work is merely "possibly piratical" (defined as giving the CBP "reasonable suspicion" that the imported work is piratical) the articles are not subject to either seizure or forfeiture, but only to detainment.[283] Next, the CBP follows a process not unlike the Notice and Takedown procedure under the DMCA. The CBP informs the importer that the material has been detained and provides the importer the opportunity to challenge the CBP's determination that the material is infringing.[284] If the importer does not respond within 30 days, the merchandise is deemed a copy and immediately becomes subject to forfeiture and seizure.[285] If the importer denies infringement, the copyright owner is informed and sent a copy of the merchandise with which to gauge if it infringes her copyright.[286] If she deems that the merchandise does in fact infringe, a proceeding is initiated and both parties have 30 days with which to submit additional evidence to the CBP for a ruling. If the merchandise is deemed non-infringing, either by Customs or the copyright owner, the merchandise is released to the importer without delay.[287]

---

280. *Id.* at 11 (noting that clearly piratical copies are "subject to seizure and forfeiture under 19 U.S.C. § 1595(c)(2)(C) for a violation of 17 U.S.C. § 602").

281. *See id.* at 8.

282. *Id.* at 8–9.

283. *Id.* at 11–12 (noting that "possible piratical copies shall be detained and the process outlined in 19 C.F.R. § 133.43 is to be followed").

284. *See id.* at 8–9.

285. *Id.*

286. *Id.* at 18.

287. *Id.* An interesting component of the Customs administrative procedures is the public's ability to help police the Internet. Currently, the CBP has an e-Allegations system where "concerned individuals can report illegal import and export activity." *Report Trade Violations—e-Allegations*, U.S. CUSTOMS & BORDER PROT., https://help.cbp.gov/app/answers/detail/a_id/1236/~/report-trade-violations---e-allegations (last visited Nov. 12, 2015). The system is intended to get as many eyes and ears on the borders as possible. While it is geared toward the "public" at large, there is speculation that Customs intends for companies to file violations when they know that their competitors "are violating trade laws or from whistleblowers within companies who know their employer is declaring a lower value for goods to avoid paying higher duties." Gautham Nagesh, *CBP Launches Online System to Report Trade Violations*, NEXTGOV (June 20, 2008), http://www.nextgov.com/health/2008/06/cbp-launches-online-system-to-report-trade-violations/42167/. The CBP permits e-Allegations to be submitted anonymously. *e-Allegations Frequently Asked Questions*, U.S. CUSTOMS & BORDER PROT., http://www.cbp.gov/trade/trade-

C. Reasonable and Effective Measures—ISP Liability

With these frameworks as background, here we sketch the contours of the duty-based system. The main thrust is that we should require ISPs to do more to prevent infringement than the current scheme. This is justified to restore the balance of the DMCA, as Congress originally envisioned, and because ISPs "control the gateway" to infringement and gain positive externalities from subscriber infringement.[288] ISPs would have an affirmative duty to monitor sites for infringing material. An ISP's duty would depend on the ISP taking reasonable and effective preventative measures to prevent copyright infringement. Because "reasonable" is a dynamic concept, the level of prevention that ISPs will be required to undertake and whether ISPs exercise reasonable care will depend on a number of factors, such as the average profits of the ISP, its percentage of the ISP market, ISP resources, the ISP's technical ability, size, and the capability and normal use of its technology system.

Reasonable measures would include notice to subscribers as to what constitutes infringement and a clear statement of a zero tolerance policy. As in the employment context, the notice requirement need not be a stringent one. YouTube's Terms of Service agreement, which provides, that the user "will not submit material that is copyrighted . . . unless [he is] the owner of such rights or ha[s] permission from their rightful owner to post the material and to grant YouTube all of the license rights granted herein" would meet any reasonableness standard.

Reasonable measures would also include methods such as monitoring, filtering, and blocking technologies, as described above. The advantage of this reasonableness standard is that it is adaptable to include newer filtering methods and other means not yet developed, accommodating and encouraging innovation. As the system will use filtering technology, copyright owners must provide ISPs with information about their copyrighted content, mirroring the CBP framework. Failure to do so will preclude any liability from attaching to ISPs. What constitutes sufficient information will depend on the type of work involved, but will generally consist of the

---

community/e-allegations/e-allegations-faqs (last visited Nov. 12, 2015). However, if an individual wishes to provide further information or evidence in the form of a photo or document, they must provide the CBP with an e-mail address in order to receive an e-Allegation case number and the address where to send the evidence. *Id.* Furthermore, for those individuals willing to provide their name and contact information with the e-Allegation, she may be entitled to a reward of 25% of what the CBP recovers, up to $250,000, if her information is significant and detailed enough. *Id.*

288. Lichtman & Posner, *supra* note 42, at 225, 258.

copyright owner's name, reference fingerprints for each media file, and for the "content owners [to] submit the business rules and metadata related to the fingerprint of each media file."[289]

The reasonableness standard is useful not only for its adaptability to different players in the field, but also its flexibility, allowing it to accommodate changing circumstances. In other words, the standard would allow for the case-by-case disposition, and gradual evolution and development of ISP liability standards that would have occurred but for the DMCA. The standard would also allow courts to adapt to the quick pace of technology, to changes in business practices, and to changes in societal norms. The standard would encourage advances in filtering technology which ultimately benefit both copyright holders and ISPs. Better technology will result in fewer infringements, while technological advances and competition should result in less costly and more efficient systems.

Two final thoughts on the duty-based regime. First, because the standard is a flexible standard it is best left to courts to develop and evolve the standard. The lone legislative action required will be to delete Section 512(m) of the DMCA (prohibiting monitoring or affirmatively seeking facts indicating infringement). Second, ISPs should be immune from liability for their good faith efforts in monitoring and filtering.[290] With this, we turn last to possible criticisms.

D. Possible Criticisms of a Duty Based Regime

The proposed liability scheme overcomes limitations of the previous proposals. Concerns relating to the prohibitive cost of any monitoring system for smaller ISPs will be allayed. A reasonableness standard protects smaller ISPs, as their resources, size, revenues, etc. are taken into consideration in determining their duties. This ensures not only that the cost for smaller ISPs will be proportional, but also that there is no disincentive for or barrier to new market entrants.[291] Also, the scheme avoids the collusive aspect of the self-governance agreements between ISPs and media.

---

289. *See* Audible Magic Brief, *supra* note 13, at 12–13.

290. *Cf.* 17 U.S.C. § 512(g)(1) (2012) ("[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.").

291. Brishen Rogers, *Toward Third Party Liability for Wage Theft*, 31 BERKELEY J. EMP. & LAB. L. 1, 49 (2010) ("By holding powerful parties to more stringent duties than weaker ones, [a duty based approach] would arguably reflect norms of fairness that often inform tort litigation.").

There are concerns. For one, a duty-based regime is inconsistent with the strict liability regimes characterized by copyright law.[292] Such a flexible standard can lead to additional litigation and the uncertainty the DMCA sought to avoid. However, as highlighted above, a dual scheme in an area of the law is not new. As the genesis of copyright secondary liability is employment law, this may not be as far a reach as it initially appears. Moreover, notably, strict liability schemes are "frankly, quite rare,"[293] and a duty based system offers advantages over strict liability systems precisely because it is flexible. It is a system that relies on a fact-sensitive, risk-utility standard of reasonableness, which might be better suited to the varied circumstances characterizing ISP liability (e.g., different users, different kinds of ISPs, and the type and extent of infringement).[294]

Granted, the duty based regime suffers the same limitations as other ex ante schemes and the problems inherent in systems relying on filtering technology (e.g., inability to account for fair/tolerated use, prior restraints, etc.). Here, I might only say that an alternative system need not be perfect—it need only be optimal and an improvement over the current system. The duty-based regime might be that.

There is another concern. If ISPs are already currently using filtering and fingerprinting technologies without any legal obligation to do so, why would there be a need to create a legal obligation? Why not let the various industries and the market continue innovating and cooperating without burdening the system with uncertainties that attend a new liability regime? One response might be that doing so will provide incentives not to the large ISPs that currently use the technology, but to the smaller ISPs who may not have the same incentives because they feel less obligated and do not face similar deterrence concerns. Here, again, the reasonableness standard would come into play.

A major fear of imposing additional liability or responsibility on ISPs is that it will result in either (or both) a detrimental impact on the future growth of the Internet or retard future innovation. Katyal and Schultz argue that current companies and innovative products would not be around but for the current scheme reflected in the DMCA. "Of the ten most visited websites in

---

292. *Id.* For an argument that copyright infringement more resembles negligence than strict liability because of the fair use defense, *see* Patrick R. Goold, *Is Liability for Copyright Infringement Strict?*, http://law.scu.edu/wp-content/uploads/Goold-Strict-Copyright-Liability-Abstract.pdf (last visited Oct. 24, 2014) ("This defense [fair use] allows the court to engage in a fine-grained factual analysis much like the concept of reasonableness in negligence.").

293. Rogers *supra* note 291, at 47.

294. *See, e.g.*, James A. Henderson, Jr., *Why Negligence Dominates Tort*, 50 UCLA L. REV. 377, 402–03 (2002).

the United States as of June 2012, five did not exist when the DMCA was passed."[295] The Internet is no longer the fledgling system it was in the 1990s. Far removed from its embryonic state, and with its far-reaching impact and still enormous growth potential, it is unlikely ISPs will shut down or fail simply because of some increased responsibility and potential liability. This is not to say that the fear is unfounded, but simply that the calculus used to evaluate and protect the Internet in 1999 is (and should be) a different calculus than the one to evaluate and protect the Internet in 2014.

Finally, we cannot evaluate an alternate scheme without considering its impact on users. The first concern here is obvious: users must still be able to access and use works in intended and permissible ways, without fear of unreasonable actions that can chill free speech and subject them to unwarranted threats. Courts and ISPs must utilize the flexibility in the proposed system to limit adverse effects. This will be on ongoing process. The second concern is targeting individuals determined to thwart the technology used in effectively policing and combating infringement. As with TPMs and other protection measures, users have devised ways to circumvent filtering systems. By way of example, one simple, yet effective method recently spread throughout the Internet community. To circumvent YouTube's Content ID system, users placed copyrighted videos inside a still photo of a cat watching television. The Content ID algorithm could not detect the copyrighted video and instead merely detected a cat watching TV.[296] The method became a popular, albeit clumsy, way to circumvent filtering and led to ridicule of any attempts at protection.[297] As one blogger noted, regardless of what technology is used to detect and prevent infringement, infringers "are continually one step ahead" and new laws and new protection methods will simply "push people to find creative new ways of getting the content they want."[298] This does not counsel for copyright owners to wave the white flag. It does mean, however, that unless there is persuasive, convincing evidence that an ex ante system (or any other system) will provide much better

295. Bryan E. Ashram, *Monetizing Infringement: A New Legal Regime for Hosts of User-Generated Content*, 101 GEO. L. J. 775, 790 n.112 (2013) ("These five are: Facebook (ranked second, created in 2004, http://www.facebook.com/facebook/info), YouTube (ranked third, created in 2005, http://www.youtube.com/t/about_youtube), Wikipedia (ranked sixth, created in 2001, http://en.wikipedia.org/wiki/Wikipedia:About), Twitter (ranked eighth, created in 2006, http://techcrunch.com/2006/07/15/is-twttr-interesting/), and LinkedIn (ranked tenth, launched in 2003, http://press.linkedin.com/about).") (citing *Top Sites in United States*, ALEXA, http://www.alexa.com/topsites/countries/US (last visited Nov. 12, 2012)).

296. Nick Bilton, *Internet Pirates Will Always Win*, N.Y. TIMES (Aug. 4, 2012), http://www.nytimes.com/2012/08/05/sunday-review/internet-pirates-will-always-win.html?_r=0.

297. *Id.*

298. *Id.*

enforcement, with less cost, and will be effective, disrupting an adequately functioning existing system should be met with some caution.

VII. CONCLUSION

Until now, the choice for ISP liability for users' infringing activities has been binary: strict liability or no liability. This need not be the case. This Article has argued that a duty-based regime layered over the current strict-liability regime might be an effective means to address copyright infringement and should be included in the debate over the optimal level of ISP liability. The new regime is justified primarily on initial congressional intent to balance the interests of copyright owners and ISPs, arguing that Congress' original effort to do so has been frustrated by unforeseen circumstances. The new regime might also be justified as a means to design a system with a mix of rules and standards that will capture some—but not all—of the types of infringement that currently lies beyond the DMCA. The system is flexible enough that it can better track the inevitable mismatch between technology and copyright law, and better respond to the ways in which technology continually affords users abilities that copyright law has not contemplated or internalized.

The Article falls short of calling for the new system to entirely replace the notice and takedown system currently in place. Rather, the Article recognizes that more data is required to make an accurate evaluation and assessment. At bottom, the question boils down to whether the alternative system will prevent more infringement, at lesser cost, without adverse and unintended consequences. This is an empirical question and the empirics are missing. Nevertheless, the system has advantages over current proposals and is worth considering alongside those.