2014

Secondary Liability, ISP Immunity, and Incumbent Entrenchment

Marketa Trimble
University of Nevada, Las Vegas -- William S. Boyd School of Law

Salil K. Mehra
Temple University - Beasley School of Law

SALIL K. MEHRA* AND MARKETA TRIMBLE**

Secondary Liability, ISP Immunity, and Incumbent Entrenchment†

TOPIC VI

More than fifteen years have passed since the two major U.S. statutes concerning the secondary liability of Internet service providers were adopted—the Communications Decency Act and the Digital Millennium Copyright Act. The statutes have been criticized; however, very little of the criticism has come from Internet service providers, who have enjoyed the benefits of generous safe harbors and immunity from suit guaranteed by these statutes. This Article raises the question of whether these statutes contribute to incumbent entrenchment—solidifying the position of the existing Internet service providers to the detriment of potential new entrants. The current laws and industry self-regulation may hamper the entry of new service providers into the market and thereby retard the technological progress that best serves society.

INTRODUCTION

Critics often view law as lagging behind technology, thereby hampering technological development and innovation. Innovators grumble that the law does not facilitate technological development—not only does it fail to anticipate future technological development, but it often is not even able to respond rapidly enough to address current developments. When innovators complain about the existing state of the law, however, their complaints might actually be a positive sign in one respect—the complaints indicate that the types of technological development are occurring that society hopes to encourage—developments that were not anticipated when the laws were drafted. If innovators are silent about or satisfied with the cur-

* James E. Beasley Professor of Law, Beasley School of Law, Temple University.

** Associate Professor of Law, William S. Boyd School of Law, University of Nevada, Las Vegas. The author would like to thank Andrew Martineau of the Wiener-Rogers Law Library for his excellent research support, and Gary A. Trimble for his superb editing advice.

† DOI: http://dx.doi.org/10.5131/AJCL.2013.0041

rent state of the law, then questions should be raised about the innovators' contributions to technological development. Technological development might not be sufficiently progressive if it corresponds exactly to what was anticipated at the time of a law's drafting by a legislature, since legislatures are bodies not typically endowed with particular technical expertise, visionary abilities, or imagination.[1]

The extremely swift development of the Internet shows how a revolutionary technology can move ahead of the law. When the new 1976 Copyright Act was enacted, only a few visionaries could have predicted the Internet's existence,[2] and even in 1996 and 1998, when Congress enacted Section 230 of the Communications Decency Act (CDA)[3] and the Digital Millennium Copyright Act (DMCA),[4] statutes that included Internet-related provisions, few could have imagined all the roles that the Internet would play and the range of legal issues that the Internet would generate in just a few years.[5] One would expect the Internet-related provisions of the CDA and the DMCA to be primary examples of how a law can lag behind technology and result in complaints by major innovators in the field about the outdated state of the law.

However, the provisions of the CDA and the DMCA that address the liability of Internet service providers (ISPs) for content posted on the Internet by third parties[6] appear to enjoy the support of ISPs,[7] which are the very same entities that society perceives to be the ma-

1. A legislature may purposefully decide not to legislate for new technologies and to delay legislating for such technologies until they are fully developed. *See* Yvette Joy Liebesman, *The Wisdom of Legislating for Anticipated Technological Advancements*, 10 J. MARSHALL REV. INTELL. PROP. L. 154, 157 (2010) ("[W]e should proceed with caution in allowing the potential effects of either technology in its infancy or future unrealized technology to influence our policy decisions before the science has had a chance to mature and develop, and its effects on society better determined." *Id.*). Of course, it might be difficult to determine when a technology has reached a proper point of maturation for a legislature to act.

2. *E.g.*, Paul Baran, *On Distributed Communications: I. Introduction to Distributed Communications Networks*, THE RAND CORPORATION (Aug. 1964), http://www.rand.org/pubs/research_memoranda/2006/RM3420.pdf. On the creation and beginnings of the Internet generally, see, e.g., JANET ABBATE, INVENTING THE INTERNET (2000); JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET—AND HOW TO STOP IT 28-35 (2008).

3. 47 U.S.C. § 230 (2006).

4. This article concerns only one set of the provisions of the DMCA—section 512—the Online Copyright Infringement Liability Limitation Act. 17 U.S.C. § 512 (2012).

5. *See, e.g.*, *In re* Verizon Internet Services, Inc., 240 F.Supp.2d 24, 38 (D.D.C. 2003) ("[P]eer-to-peer (P2P) software and 'bots,' a software tool used by copyright owners to monitor the Internet and detect unauthorized distribution of copyrighted material—were 'not even a glimmer in anyone's eye when the DMCA was enacted' by Congress in 1998." *Id.*).

6. 17 U.S.C. § 512 (2012).

7. *See infra* note 16 and note 103 and the accompanying text for the scope of the term "Internet service providers" under the DMCA and the CDA.

jor innovators of the Internet.[8] The CDA and the DMCA are two of the three U.S. federal acts that limit the liability of ISPs[9]—persons or entities that facilitate Internet connections and a wide variety of other Internet-related services, such as search functions (e.g., Google) and platforms for posting of content created by others (e.g., YouTube). The provisions of the acts immunize ISPs from suit and create safe harbors from some types of remedies in cases where ISP liability would or does arise because of acts by users employing ISP services—acts that are facilitated by the ISP services and that involve illegal conduct, such as defamation or copyright infringement.[10]

The fact that ISPs appear to be satisfied with the CDA and the DMCA as they have existed since 1996 and 1998 does not automatically mean that ISPs do not innovate at all, or do not innovate sufficiently in the technology that the CDA and the DMCA affect; good examples exist of innovation by some ISPs in technological aspects that are affected by the CDA and the DMCA.[11] But ISP satisfaction with the law might also suggest that the law does not adequately incentivize ISPs to innovate in particular aspects of technology, and in the worst case scenario, the law could actually incentivize ISPs to slow their innovation in technology, or constantly understate the outcomes of their innovation in particular technologies that are implicated by the CDA and the DMCA.

The CDA and the DMCA were designed to support the development of a new and promising industry,[12] and the immunity provided

---

8. *E.g.*, 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." David Goldman, *Google Kills 250,000 Search Links A Week*, CNN MONEY (Sept. 9, 2013), http://money.cnn.com/2012/05/24/technology/google-search-copyright. On criticism of the DMCA by users, free speech advocates, and copyright owners *see, e.g.*, Jennifer M. Urban & Laura Quilter, *Efficient Process or "Chilling Effects"? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 621, 631–36 (2006); Rebecca Tushnet, *Power Without Responsibility: Intermediaries and the First Amendment*, 76 GEO. WASH. L. REV. 986, 1002–05 (2008); Wendy Seltzer, *Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment*, 24 HARV. J.L. & TECH. 171 (2010); CHILLING EFFECTS, http://www.chillingeffects.org (last visited Sept. 20, 2013).

9. The third (less known) act is the Lanham Act. 15 U.S.C. § 1114(2)(B), (C) (2006).

10. For the scopes of the safe harbor and immunization provisions see *infra* note 15 and the accompanying text and notes 92, 104, 105, and the accompanying texts.

11. *See infra* for examples of technologies deployed by ISPs to enhance copyright enforcement. Innovation in the technologies may be conducted by entities other than ISPs—by third-party suppliers of the technologies, for example. ISP demand for such technologies plays an important role in incentivizing suppliers to innovate, and ISP demand can be propelled by legal requirements. For simplification this article identifies ISPs as the primary innovators with the understanding that innovation may be outsourced to third-party suppliers.

12. "The history of online gatekeeping is . . . also one of policy judgment in the judicial as well as legislative spheres that generative technologies ought to be given

by CDA's Section 230 and the safe harbor provided by the DMCA to internet service providers were critical to the early development of the Internet. However, the CDA and the DMCA may also be contributing to some ossification in the forms that subsequent Internet services may take. Additionally, the newly-implemented Copyright Alert System (also known as "six strikes") may, through self-regulation, provide incumbent firms with advantages that will burden insurgent innovators.

I. THE DIGITAL MILLENNIUM COPYRIGHT ACT

The status of ISPs and their potential liability for content posted on the Internet by third parties, particularly for defamatory and copyright infringing content, has been contested in courts since the early days of the Internet, and as courts reached different results on the status of ISPs,[13] an urgent need for legal certainty led Congress to enact first Section 230 of the CDA, and later the DMCA, which filled the gap that the CDA purposefully left in the copyright law area. The DMCA reflected a pushback by copyright owners, who demanded that ISPs be required to meet certain conditions to benefit from a limitation on ISP liability, and that a mechanism be created for takedowns of copyright infringing material.[14] The DMCA's safe harbor provisions concern liability for copyright infringement that may arise under the U.S. Copyright Act,[15] and provide specifically defined ISPs only a safe harbor from damages, not complete immunity from suit.[16]

---

wide latitude to find a variety of uses . . ." Jonathan Zittrain, *A History of Online Gatekeeping*, 19 HARV. J. L. & TECH. 253, 298 (2006). *See also* 144 Cong. Rec. S8729 (daily ed. Sept. 3, 1997) (statement of Sen. Ashcroft) ("We cannot make the Internet too costly to operate.").

13. *E.g.*, Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135, (S.D.N.Y. 1991); Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995).

14. In re Verizon Internet Services, Inc., 240 F.Supp.2d 24, 36 (D.D.C. 2003) ("The legislative history makes clear that in enacting the DMCA, Congress attempted to balance the liability protections for service providers with the need for broad protection of copyrights on the Internet." *Id.*).

15. 17 U.S.C. § 512 (2012). Courts disagree on whether the DMCA extends to secondary liability that may arise under state copyright laws. *See* Capitol Records, Inc. v. MP3tunes, LLC, 821 F. Supp. 2d 627 (S.D.N.Y. 2011); UMG Recordings, Inc. v. Escape Media Grp., Inc., 964 N.Y.S.2d 106 (2013). *See also Federal Copyright Protection for Pre-1972 Sound Recordings, A Report of the Register of Copyrights, December 2011*, U.S. COPYRIGHT OFFICE, http://www.copyright.gov/docs/sound/pre-72-report.pdf (last visited Aug. 22, 2013). It is also questionable whether the DMCA covers secondary liability if such liability arises under anti-circumvention provisions of the U.S. Copyright Act. *See* 17 U.S.C. § 1201 (2006). It is disputed whether the provision creates secondary liability. Mark A. Lemley, *Rationalizing Internet Safe Harbors*, 6 J. TELECOMM. & HIGH TECH. L. 101, 107 (2007).

16. The safe harbor provisions of the DMCA are limited to service providers of "digital online communications" and providers "of online services or network access, or the operator of facilities thereof" who fall into one of four categories. 17 U.S.C. § 512(k)(1)(A) and (B) (2012). For the individual categories see 17 U.S.C. § 512(a), (b),

Among the requirements that ISPs must fulfill to benefit from the DMCA safe harbor is, for some categories of ISPs,[17] compliance with a mechanism for taking down allegedly copyright infringing material. The DMCA outlines the mechanism in great detail; it specifies the content for notifications that copyright owners must submit to ISPs if the copyright owners want the ISPs to take down allegedly infringing material,[18] it details the counter-notifications that users may file to defend material that they upload,[19] and it outlines ISP takedown and reinstatement actions.[20] The mechanism operates on two premises: first, that ISPs do not have the technical means to police content that third parties upload to the Internet and that the ISPs host or link to, and second, that even if ISPs have those means, the ISPs are not able to assess whether or not particular material is copyright infringing because they lack basic information necessary for such an assessment, including information about the current copyright owner of the material and any licensing arrangements into which the copyright owner might have entered.

The same two premises that underlie the takedown mechanism also underlie another requirement—the absence of a certain degree of knowledge about infringing activity. If an ISP has such knowledge, the ISP will not benefit from the DMCA safe harbor.[21] Much DMCA-related litigation[22] has focused on the gap between 1) the knowledge

---

(c), and (d). *See also* Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102 (9th Cir. 2007); Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19 (2d Cir. 2012); UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006 (9th Cir. 2013); Columbia Pictures Indus., Inc. v. Fung, 710 F.3d 1020 (9th Cir. 2013) (deciding that BitTorrent sites were not covered by 17 U.S.C. §512(a), (b) and (d)). The DMCA also has a special provision for nonprofit educational institutions acting as service providers. 17 U.S.C. §512(e) (2012).

17. 17 U.S.C. §512(c) and (d) (2012).

18. 17 U.S.C. §512(c)(3) (2012).

19. 17 U.S.C. §512(g)(3) (2012).

20. 17 U.S.C. §512(g)(2) (2012).

21. The absence of knowledge requirement also concerns only ISPs under 17 U.S.C. § 512(c) and (d).

> [T]he 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; . . .

17 U.S.C. § 512(c)(1)(A) (2012).

22. In addition to the issues related to the actual knowledge requirement and the "right and ability to control" infringing activity, DMCA-related litigation has concerned issues such as compliance with the definition of ISPs covered by the DMCA, the requirements for the repeat infringer policy, and personal jurisdiction over a copyright owner based on the filing of a DMCA notification. *See* cases listed *supra* in note 16; Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1109-15 (9th Cir. 2007); Dudnikov v. Chalk & Vermilion Fine Arts, Inc., 514 F.3d 1063 (10th Cir. 2008).

that the DMCA requires the ISP not to have,[23] and 2) the knowledge that the ISP undeniably has once it receives a DMCA notification from a copyright owner. ISPs, understandably, want no gap to exist between the two; for ISPs the ideal situation is one in which no actual or "red flag" knowledge is imputed to them unless they receive a DMCA notification from a copyright owner containing all the information that the law requires.[24] Copyright owners, however, want not only for a gap to exist, but that the gap be as wide as possible; a level of knowledge much lower than knowledge based on a DMCA notification should suffice, according to them, for ISPs to be presumed to have sufficient knowledge of infringement, be outside of the DMCA safe harbor, and be fully liable for secondary copyright infringement.[25] Discussions continue to surface about the state of technology that is available to ISPs and the potential ability of ISPs to identify allegedly infringing material without a DMCA notification from a copyright owner.

The availability of technology that might assist ISPs in identifying potentially infringing material has been the subject of debate since the DMCA was drafted.[26] Other arguments as to why ISPs are ill-suited to identify and remove content that allegedly infringes copyright have also appeared in the debates—lack of sufficient information, privacy concerns, the danger of over-enforcement,[27] and technological limitations have all been argued. The legislative history of the DMCA shows that in the legislative process ISPs emphasized their technological limitations, which they said prevented them from monitoring content for allegedly copyright infringing material. In a Senate committee hearing, an AOL executive, for example, argued that an ISP's "duty to act, and to be liable, should be triggered only when it has actual knowledge of the infringement, and where it is *technically and legally feasible and economically reasonable*, to remove or stop it."[28] He warned that although technological means were in development, they were "still in their nascent development stage" and "not likely to be ready for deployment for several years."[29]

A concern that surfaced even in the legislative process was that by following the then-current state of technology the DMCA would

23. *Supra* note 21.

24. *Supra* note 18. *See, e.g.*, Columbia Pictures Indus., Inc. v. Fung, 710 F.3d 1020, 1043 (9th Cir. 2013).

25. *See, e.g.*, Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 31 (2d Cir. 2012); UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006, 1022 (9th Cir. 2013).

26. 144 Cong. Rec. S8729 (daily ed. Sept. 3, 1997) (statement of Sen. Ashcroft) (discussing "the capabilities and limits of current technology").

27. *E.g.*, *Copyright Infringement Liability of Online and Internet Service Providers: Hearing on S. 1145 Before the S. Comm. on the Judiciary*, 105th Cong. 32 (1997) (statement of Roy Neel, Pres. and CEO of the U.S. Telephone Association).

28. *Id.* at 27 (statement of George Vradenburg, III) (emphasis added).

29. *Id.* at 87 (responses of George Vradenburg, III to questions from Sen. Leahy).

not provide sufficient incentives for ISPs to 1) innovate in the detection of allegedly copyright infringing material, and 2) deploy such technology once it was developed. Although copyright owners agreed with the ISPs that combating copyright infringement online would need to be a team effort by ISPs and copyright owners, they wanted more responsibility to be shifted to ISPs and the legislation to incentivize ISPs to innovate.[30] During a Senate committee hearing the General Counsel of the Recording Industry Association of America referred to technological solutions as the achievable "holy grail"[31] and questioned the wisdom of limiting ISP liability: "[I]f the [ISPs] got their way and got [the] exemption from liability, then what would be their incentive to deploy the technology?"[32] "The more . . . ISPs are insulated from copyright liability," an attorney representing the Motion Picture Association of America warned, "the less incentive they will have to cooperate with copyright owners to protect their works."[33] ISPs countered by declaring their commitment to innovation; they argued that because the legislation focused on defining the absence of knowledge requirement rather than on introducing a technology-specific standard, the legislation would grow with technological development and not hamper industry development.[34]

The effects of the DMCA safe harbor provisions on ISP innovation have not been as grim as some copyright owners feared; ISPs have not stopped innovating in the area of content identification, and some have taken steps to assist in fighting copyright infringement on the Internet that have gone beyond the letter of the DMCA. Some ISPs have provided content identification tools to copyright owners to enable them to enhance the copyright owners' ability to identify allegedly infringing materials in order to file DMCA notifications. For example, YouTube has provided copyright holders with "Content ID"—a tool that copyright holders can use to identify and manage potential copyright infringements.[35] The tool compares videos uploaded to YouTube "against a database of files that have been submitted to [YouTube] by content owners," and "[w]hen Content ID identifies a match between [a right holder's] video and a file in this

30. *Id.* at 67 (responses of Fritz Attaway to questions from Sen. Hatch) ("Technology will likely provide the tools by which . . . ISPs and content owners, working together, develop and implement efficient and effective method to discover and eliminate infringing activities.").

31. *Id.* at 40 (statement of Cary H. Sherman, Senior Executive Vice President and General Counsel of the RIAA).

32. *Id.*

33. *Id.* at 68 (responses of Fritz Attaway to questions from Sen. Hatch).

34. *Id.* at 87 (responses of George Vradenburg, III to questions from Sen. Leahy).

35. *How Content ID Works*, YOUTUBE, https://support.google.com/youtube/answer/2797370?p=cid_what_is&rd=1 (last visited Sept. 23, 2013). For criticism of YouTube's delaying the deployment of the technology see Opening Brief for Plaintiffs-Appellants at 13, 37, 45, Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19 (2nd Cir. 2012) (No. 10-3270), 2010 WL 4930315.

database, it applies the policy chosen by the content owner."[36] Other ISPs have deployed tools that are designed to identify and remove potentially copyright infringing material. For example, Veoh introduced "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.[37] Veoh has also utilized "fingerprinting" technology by a third-party supplier, Audible Magic, to identify potentially copyright infringing content that Veoh either removes or refuses to post.[38]

What has propelled the development of the technologies if the law provides no incentives to innovate in the technologies? As some predicted, the need to maintain good relations with content providers has driven ISPs to cooperate voluntarily with copyright owners.[39] The technologies may also serve copyright owners indirectly because information about patterns of copyright infringement on the Internet can be helpful to content providers that seek to identify material that is in demand and therefore attractive for companies to offer to users legally.[40] Reasons other than detecting copyright infringement also generate interest in the development of content identification technologies,[41] and copyright owners' lawsuits against and financial investments in ISPs also prompt a more widespread adoption of the technologies.[42]

It is important for the development of the technologies that courts have not penalized ISPs for their voluntary implementation of

---

36. *Id.* The policies that the copyright owner may choose are labeled as "monetize," "block," and "track." *Id.*

37. UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006, 1012 (9th Cir. 2013).

38. *Id.*, pp. 1012-13. *See* Audible Magic, http://audiblemagic.com/ (last visited Sept. 23, 2013). "This filtering occurs even if Veoh never received a DMCA notice regarding the video." Brief of Appellee Veoh Networks at 13, UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006 (9th Cir. 2013) (Nos. 09-55902, 09-56777, 10-55732), 2010 WL 3706519. Veoh was criticized because it had not deployed the available technologies earlier. *See* Appellants' Brief at 63-64, UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006 (9th Cir. 2013) (Nos. 09-55902, 09-56777, 10-55732), 2010 WL 3706518.

39. *Copyright Infringement Liability of Online and Internet Service Providers: Hearing on S. 1145 Before the S. Comm. on the Judiciary*, 105th Cong. 87 (1997) (responses of George Vradenburg, III to questions from Sen. Leahy).

40. Mark Leiser, *Netflix Admits Using Pirate Sites to Determine What Content to License*, THE DRUM (Sept. 14, 2013), *available at* http://www.thedrum.com/news/2013/09/14/netflix-admits-using-pirate-sites-determine-what-content-license.

41. *See, e.g.*, Gracenote MusicID®, http://www.gracenote.com/music/recognition/ (last visited Sept. 26, 2013); Jason Papanicholas, *Top 5 Apps for Identifying Songs*, EVOLVER.FM (Oct. 12, 2012), http://evolver.fm/2012/10/10/top-5-apps-for-identifying-songs.

42. *See* Reply Brief of Appellants at 12, UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006 (9th Cir. 2013) (Nos. 09-55902, 09-56777, 10-55732), 2010 WL 3708631 (Veoh "only started screening [content] when a later investor, Time Warner, insisted that this be done as a condition of its investment.").

content identification technologies. For example, courts have not imputed actual or "red flag" knowledge to ISPs simply because the ISPs have used the technologies, or have had the technologies available and chose not to use them. In a case involving Veoh, the U.S. Court of Appeals for the Ninth Circuit refused to impute such knowledge to Veoh, reiterating that "the DMCA recognizes that service providers who do not locate and remove infringing materials they do not *specifically* know of should not suffer the loss of safe harbor protection."[43] As the U.S. Court of Appeals for the Second Circuit stated in a case involving YouTube, "the nature of the removal obligation itself contemplates knowledge or awareness of specific infringing material."[44] Courts have also required "something more than the ability to remove or block access to materials posted on a service provider's website"[45] for a finding of the "right and ability to control"[46] that, combined with "a financial benefit directly attributable to the infringing activity,"[47] would also make ISPs ineligible for the DMCA safe harbor. In the Veoh case the Ninth Circuit Court confirmed that Veoh's use of technologies to identify and remove allegedly copyright infringing material was "not equivalent to the activities found to constitute substantial influence"[48] on users' activities, and therefore the use of the technologies did not constitute a "right and ability to control" infringing activities.[49] Therefore the fact, by itself, that technology was available to an ISP to identify allegedly infringing material did not take the ISP outside the DMCA safe harbor—even when the ISP failed to use the technology (or failed to use it sufficiently).

Of course, copyright owners have campaigned for greater ISP responsibility in combating copyright infringements and a requirement for increased ISP use of technologies to identify and remove copyright infringing content—technologies that copyright owners insist have been available for some time.[50] Copyright owners have accused ISPs of purposefully avoiding or delaying the deployment of technologies in order to make their services more appealing by making them avail-

43. UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006, 1020 (9th Cir. 2013) (emphasis added).

44. Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 30 (2d Cir. 2012).

45. *Id.* at 38.

46. 17 U.S.C. § 512(c)(1)(C) and (d)(2) (2012).

47. *Id.*

48. UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006, 1030 (9th Cir. 2013).

49. *Id.*

50. *E.g.*, Brief of Appellants at 20-21, UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006 (9th Cir. 2013) (Nos. 09-55902, 09-56777, 10-55732), 2010 WL 3708623; Appellants' Brief at 21, UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006 (9th Cir. 2013) (Nos. 09-55902, 09-56777, 10-55732), 2010 WL 3706518.

able for copyright infringing activities.[51] Further, copyright owners have argued that because technologies have been available, ISPs "could have identified [copyright infringing] material by filtering or otherwise searching [their] system[s],"[52] and because ISPs have had the capability to remove such material, they should have been held to have had sufficient "red flag" knowledge and the "right and ability to control" the infringing activities of their users.

Courts have not agreed with copyright owners' calls for greater ISP responsibility in combating online copyright infringements and have not required ISPs to use available technologies to enhance copyright enforcement on the Internet. However, courts have adopted an approach to the absence of knowledge requirement and to the absence of the "right and ability to control" requirement that will not motivate ISPs to discontinue innovating various technologies that would help combat copyright infringements. Consider the potential outcome if courts were to adopt the opposite approach, i.e. if courts decided that the mere availability of a technology capable of identifying allegedly infringing content would be enough to cause ISPs to have a sufficient level of "red flag" knowledge and/or the "right and ability to control" infringing activity. In such a case the existence of the knowledge or the "right and ability to control" would take ISPs out of the DMCA safe harbor and therefore make it unappealing for ISPs to develop and utilize new technologies. Courts have avoided this undesirable result that commentators had feared would occur because the DMCA's absence of knowledge requirement indeed appeared to be rewarding ISPs who are not deploying technologies that would assist in identifying infringing material.[53]

Although case law developed so that the law does not *penalize* ISPs for deploying the technologies, the statute and case law do nothing to *prompt* ISPs to innovate. The DMCA includes a requirement that ISPs "accommodate[. . .] and do[. . .] not interfere with standard technical measures,"[54] but it does not require ISPs to actively seek technologies that would assist in combating copyright infringe-

51. *E.g.*, Opening Brief for Plaintiffs-Appellants at 13, 37, 45, Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19 (2nd Cir. 2012) (No. 10-3270), 2010 WL 4930315; Brief of Plaintiffs-Appellees at 14, Columbia Pictures Indus., Inc. v. Fung, 710 F.3d 1020 (9th Cir. 2013) (No. 10-55946), 2011 WL 2191541 (pointing out that the defendants did not use the available technologies to identify and remove copyright infringing content although they did use the technologies to eliminate pornography); Brief of Appellants at 21, 49, UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006 (9th Cir. 2013) (Nos. 09-55902, 09-56777, 10-55732), 2010 WL 3708623.

52. Appellants' Brief at 67, UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006 (9th Cir. 2013) (Nos. 09-55902, 09-56777, 10-55732), 2010 WL 3706518.

53. Zittrain, *supra* note 12, at 292.

54. 17 U.S.C. § 512(i)(1)(B) (2012).

ments.[55] Currently, copyright owners are not lobbying for changes in the statute that would place greater responsibility on ISPs and create incentives for ISP innovation in copyright enforcement-related technologies. Given the highly negative public reactions to recent enforcement campaigns by large copyright owners and also to legislative attempts to enhance copyright enforcement on the Internet,[56] it is not surprising that copyright owners have made a strategic decision to emphasize the need for more voluntary initiatives by ISPs rather than to push for changes to ISP legal obligations under the DMCA.[57]

The situation in the United States is interesting from a comparative perspective.[58] Other countries have adopted various versions of limitations of ISP liability, even though no agreement on the parameters of the limitations has ever been reached at the international level.[59] Countries attempted and failed to agree on the parameters, so it is likely that they will return to negotiations of conditions of ISP liability in the near future.[60] For now, countries' laws differ in the details of their approaches to ISP liability; other countries' statutes are far less detailed regarding the parameters of ISP liability than the DMCA is in the United States. For example, the European Union's E-Commerce Directive includes four articles on ISP liability[61] but does not go into the level of detail that the DMCA does.

---

55. The DMCA includes a provision that states that "[n]othing in [section 512] shall be construed to condition the applicability of subsections (a) through (d) on . . . a service provider monitoring its service or affirmatively seeking facts indicating infringing activity . . ." 17 U.S.C. § 512(m) (2012).

56. *See, e.g.*, Stop Online Piracy Act, H.R. 3261, 112th Cong. § 102(c)(4)(A)(ii) (2011). *See also* the reactions to the negotiations of the Anti-Counterfeiting Trade Agreement, May 2011, http://www.mofa.go.jp/policy/economy/i_property/pdfs/acta1105_en.pdf (last visited Sept. 24, 2013).

57. *RIAA CEO to Tout Voluntary Anti-Piracy Initiatives as Way Forward, Calls on Search Engines to Join the Effort Asks Congress to Facilitate Discussion on DMCA in Testimony Before House Panel*, RIAA (Sept. 18, 2013), https://www.riaa.com/newsitem.php?content_selector=newsandviews&news_month_filter=9&news_year_filter=2013&id=B6D2A187-624C-2A95-F8D2-70D07F0B10FA.

58. For a recent comparative discussion of the DMCA see, e.g., Dennis S. Karjala, *International Convergence on the Need for Third Parties to Become Internet Copyright Police (But Why?)*, 12 RICH. J. GLOBAL L. & BUS. 189 (2013).

59. *Cf.* Agreed Statements Concerning the WIPO Copyright Treaty, Dec. 20, 1996, Concerning Article 8. *See also* Internet Intermediaries and Creative Content, WIPO, http://www.wipo.int/copyright/en/Internet_intermediaries/ (last visited Sept. 23, 2013).

60. Choice of law issues on the Internet and the resulting uncertainty about which country's laws govern ISP secondary liability may make an agreement about an internationally harmonized standard for ISP liability particularly pressing. *See, e.g.*, Graeme B. Dinwoodie, Rochelle Dreyfuss & Annette Kur, *The Law Applicable to Secondary Liability in Intellectual Property Cases*, 42 N.Y.U. INT'L L. & POL. 201 (2009).

61. Directive 2000/31 of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market ("E-Commerce Directive"), art. 12-15, 2000 O.J. (L 178) (EC).

Although the Directive sets out an obligation for ISPs to remove or disable access to certain material upon obtaining actual knowledge of certain facts,[62] it does not include provisions on the required level of knowledge and does not outline a mechanism for a takedown procedure. The lack of details in national implementing provisions has frustrated ISPs; some ISPs have litigated cases filed against them in individual countries in order to obtain more guidance regarding ISP obligations under a country's laws.[63]

Recent decisions by the German Supreme Court have shed light on the implementation of ISP liability provisions in Germany and the requirements that German law imposes on ISPs if they want to be shielded from liability for user content. The decisions arose from two cases that concerned RapidShare, an online file storage provider, and raised the question of how much monitoring, if any, an ISP should be required to conduct in order to be shielded from liability for user content. Similarly to the DMCA,[64] the E-Commerce Directive prohibits European Union member states from "impos[ing] a general obligation on [ISPs] to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity."[65] The Court of Justice of the European Union has reiterated and clarified the prohibition of general monitoring in its recent decisions, in which the Court held court-imposed, time-unlimited, general filtering to be in violation of the European Union Charter of Fundamental Rights and other EU legislation, including the E-Commerce Directive.[66] However, the Directive leaves room for member states to specify in their national law a requirement for ISPs to "apply duties of care, which can reasonably be expected from [ISPs] . . . , in order to detect and prevent certain types of illegal activities."[67] It was the nationally imposed "duty of care" that was contested in the RapidShare cases; RapidShare insisted that it was unable to identify potentially copyright infringing content and there-

62. *Id.*, Articles 13(1)(e) and 14(1)(b).

63. *E.g.*, Landgericht Hamburg [LG Hamburg] [District Court of Hamburg] Apr. 20, 2012, 310 O 461/10, 2012 (Ger.). *See also* Rita Matulionyte, Sylvie Nerisson, *The French Route to an ISP Safe Harbour, Compared to German and U.S. Ways*, 42 IIC 55, 63 (2011) (discussing differences among ISP liability standards in European Union's member states). Eventually courts will also have to address difficult choice of law issues concerning ISP liability. For discussions of choice of law and ISP liability see *supra* note 60. *See also* proposals for resolving the choice of law issues in AM. LAW INST., INTELLECTUAL PROP.: PRINCIPLES GOVERNING JURISDICTION, CHOICE OF LAW, AND JUDGMENTS IN TRANSNATIONAL DISPUTES (2008); CONFLICT OF LAWS IN INTELLECTUAL PROPERTY: THE CLIP PRINCIPLES AND COMMENTARY (2013).

64. 17 U.S.C. § 512(m) (2012).

65. E-Commerce Directive, *supra* note 61, Article 15(1).

66. Case C-70/10, Scarlet Extended SA v. Société Belge des Auteurs, Compositeurs et Éditeurs SCRL (SABAM), 2011 E.C.R. I-11959 ; Case C-360/10, Belgische Vereinigung van Auteurs, Componisten en Uitgevers (SABAM) v. Netlog NV, 2012 ECJ EUR-Lex LEXIS 277 (Feb. 16, 2012).

67. E-Commerce Directive, *supra* note 61, recital 48.

fore could not be required to monitor content that its users uploaded to its service.[68]

In RapidShare's first litigation the appellate court, the Düsseldorf Oberlandesgericht, recognized that the ISP was obligated to take down material once the ISP was notified by a right owner that particular material was infringing the right,[69] and also to take reasonable measures to prevent future infringements.[70] However, the court rejected the argument that the ISP could have any obligation to monitor content generally, without a notification from a right holder about specific infringing material. The court pointed out the technical inability of the ISP to automate such monitoring, including the inability of ISPs to review encrypted content,[71] and the potential intensity of resource use if monitoring were conducted manually.[72] But the German Supreme Court disagreed with the appellate court;[73] it emphasized that while an obligation cannot be imposed to monitor content generally, ISPs have an obligation to monitor content in "specific cases"[74] once a right owner notifies them of infringement,[75] which includes monitoring of future infringements of the same content.[76] The court held that an ISP will be liable if the ISP receives such a notification and does not do "everything that is for the ISP technically and economically reasonable to prevent further infringements."[77]

In the second RapidShare decision the Supreme Court was even stricter than it was in the first case;[78] the Court explained that the monitoring role of an ISP might be even greater if the ISP promotes

68. Oberlandesgericht Düsseldorf [OLG] [Düsseldorf Court of Appeals] Dec. 21, 2010, I-20 U 59/10, 2010 (Ger.). The liability at issue was the so-called "Störerhaftung." *See* Jan Bernd Nordemann, *Internet Copyright Infringement: Remedies Against Intermediaries—The European Perspective on Host and Access Providers*, 59 J. COPYRIGHT SOC'Y U.S.A. 773, 782-84 (2012). *See also* Case C-324/09, Opinion of Advocate General Jääskinen, L'Oréal v. eBay, 2011 E.C.R. I-06011, at par. 56 and fn. 31.

69. Oberlandesgericht Düsseldorf, I-20 U 59/10, Dec. 21, 2010, par. 24, quoting Oberlandesgericht Düsseldorf, I-20 U 166/09, Apr. 27, 2010.

70. *Id.* at par. 24, quoting Oberlandesgericht Düsseldorf [OLG] [Düsseldorf Court of Appeals] Apr. 27, 2010, I-20 U 166/09, 2010 (Ger.).

71. *Id.* at par. 34, quoting Oberlandesgericht Düsseldorf [OLG] [Düsseldorf Court of Appeals] Apr. 27, 2010, I-20 U 166/09, 2010 (Ger.).

72. *Id.* at par. 30, quoting quoting Oberlandesgericht Düsseldorf [OLG] [Düsseldorf Court of Appeals] Apr. 27, 2010, I-20 U 166/09, 2010 (Ger.).

73. Bundesgerichtshof [BGH] [Federal Court of Justice] July 12, 2012, I ZR 18/11, 2012 (Ger.).

74. *Id.* at par. 19.

75. *Id.* at par. 28.

76. On the need to achieve "takedowns that don't automatically repopulate" see Cary H. Sherman, Senior Executive Vice President and General Counsel of the RIAA, Hearing before the Committee on the Judiciary (Sept. 18, 2013), http://www.ustream.tv/recorded/38936315 (last visited Sept. 25, 2013), at 50:26 and ff.

77. Bundesgerichtshof [BGH] [Federal Court of Justice] July 12, 2012, I ZR 18/11, 2012 (Ger.) at par. 31.

78. Bundesgerichtshof [BGH] [Federal Court of Justice] Aug. 15, 2013, I ZR 80/12, 2013 (Ger.).

copyright infringement by its users.[79] Because the lower court had established in the second case that RapidShare did promote infringements by its users and benefited financially from the influx of users seeking to use its services in copyright infringing manners, the Court held that RapidShare was required to monitor content uploaded by its users.[80] The Court did not consider the "general organizational measures"[81] that the defendant introduced to be sufficient,[82] and affirmed the lower court decision imposing a "general 'market watching obligation,'"[83] which the Court deemed appropriate given the nature of the defendant's business model.[84]

The difference between the results in the two German cases and the situation under the DMCA is remarkable. Under the DMCA, RapidShare would probably benefit from the safe harbor[85] and therefore not be required to monitor user content. Of course an ISP's promotion of infringing activity might lead to a finding of inducement of copyright infringement in the United States. But the DMCA alone would not require an ISP to introduce technologies to identify any content that was potentially copyright infringing, and to avoid inducement, an ISP would also not have to introduce any monitoring. In this sense German law appears to incentivize ISP innovation more than U.S. law does because the German Supreme Court requires more technology from ISPs than U.S. courts do.[86] Less legislative guidance in Germany seems to allow German courts to adjust technology requirements based on the current state of technology and respond to the development of technology and business models. This result is an interesting example that defies some key comparative law stereotypes: Typically, the statute of a civil law country would be expected to be more detailed than the statute of a common law country, and

79. *Id.* at par. 36.

80. *Id.* at par. 39.

81. *Id.* at par. 50.

82. These measures included the creation of a special "Abuse Team" to monitor potential infringements, introduction of a new provision in the user agreement to warn users that copyright infringements were not permitted, deployment of MD5 filters, and providing copyright owners with an interface to locate potentially infringing material. *Id.*, par. 51-54.

83. *Id.* at par. 60.

84. *Id.* at par. 62.

85. In Perfect 10 v. RapidShare, 3:09-cv-02596-H-WMC (S.D. Cal. May 18, 2010), the court concluded that "RapidShare [was] not likely to succeed on its DMCA affirmative defense" but the reason in this case was that RapidShare did not designate an agent with the U.S. Copyright Office as required by the DMCA and thus did not meet the requirements of the DMCA safe harbor. 17 U.S.C. § 512(c)(2). Since RapidShare remedied this omission it could probably benefit from the DMCA safe harbor. *See DMCA Agent*, RAPIDSHARE, https://rapidshare.com/help/dmca (last visited Sept. 25, 2013).

86. *See also* Karjala, *supra* note 58, at 210 ("[T]he obligation [imposed by the German Supreme Court] is more than has been required of ISP under section 512 by the U.S. courts.").

civil law courts would be expected to be less engaged in "legislating" than common law courts when interpreting and applying statutes.

The effects of the two German Supreme Court decisions have yet to be assessed. The effects should transcend the original litigation, because although the decisions of the Supreme Court are without precedential power *de jure, de facto* they provide guidance for lower courts and thus also *de facto* case law for the norms that govern ISPs. It is possible that the second holding will be understood to be limited to ISPs who actively promote infringements by their users, but it is also possible that German courts will begin to examine ISP deployment of content identification technologies (short of general monitoring) as one factor in assessing whether ISPs should be held liable for user content.

There is no doubt that the DMCA has played an important role in the development of the Internet industry and that it has helped to create an environment that generates a great deal of Internet-related innovation; some technologies and business models might have not have been developed without the DMCA. However, the DMCA provides no incentives for ISPs to discover particular instances of infringements; although the DMCA, as it has been applied in courts, does not discourage ISPs from developing technologies that can assist in identifying infringing material, it provides no incentives for ISPs to do so.[87] Of course it might be difficult to adjust the DMCA or court interpretations of the statute to create such incentives; the approach taken by the German Supreme Court has yet to be tested. Voluntary initiatives by ISPs who strive to assist copyright owners in combating copyright infringements are commendable; the question is whether the technological developments that the initiatives represent are sufficient and sustainable. Missed developments in new technologies may be troubling for other reasons in addition to the need for copyright enforcement;[88] the same technologies could help create and support the functioning of what has been referred to as the "celestial jukebox"—an on-demand service securing access to all copyrighted works from anywhere in the world for a fee; this service would be the ultimate solution to the problems of transaction costs and potential underutilization of copyrighted works.[89]

---

87. Zittrain, *supra* note 12, p. 292.

88. *See* Brief of Amici Curiae Stuart N. Brotman, Ronald A. Cass, and Raymond T. Nimmer in Support of Plaintiffs-Appellants at 18-21, Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19 (2nd Cir. 2012) (No. 10-3270), 2010 WL 5167429 (explaining that an ISP, such as YouTube, is in the best position to locate and remove copyright infringing material); Nicholas W. Bramble, *Safe Harbors and the National Information Infrastructure*, 64 HASTINGS L.J. 325, 351-54 (2013) (discussing why technological solutions implemented by ISPs would be beneficial).

89. Paul Goldstein, COPYRIGHT'S HIGHWAY: FROM GUTENBERG TO THE CELESTIAL JUKEBOX 28-29 (1994). Paul Goldstein has claimed no credit for the celestial jukebox metaphor.

II. SECTION 230 OF THE COMMUNICATIONS DECENCY ACT

Section 230 of the Communications Decency Act is often celebrated as one of the most valuable tools for protecting freedom of expression and innovation on the Internet. Certainly, Section 230 has created a liability shield that has allowed for YouTube and Vimeo users to upload their own videos, Amazon and Yelp to provide massive numbers of (often scathing) user reviews, and Facebook and Twitter to offer social networking services to a large portion of the world's population. And the fact that Canada, Japan, and many European nations do not have exactly equivalent statutes[90] helps explain in part why most prominent online services are based in the United States. Nonetheless, as will be explained, like the DMCA, the CDA may in fact play a role in ossifying the structure of Internet services.

Admittedly, the immunity that the CDA provided to ISPs and other service providers was important to their development. Section 230 was enacted in order to provide legal certainty to ISPs that they would not have to engage in onerous supervision of their customers' content or else face liability; the fact that this proposition was not previously free from doubt threatened to inhibit nascent Internet-based firms.[91] Section 230 immunizes or provides safe harbors to Internet service providers from liability for the conduct of others.[92] In 1996 the CDA codified an approach to secondary liability that courts had established prior to the enactment of the CDA; the approach held that conduits were not secondarily liable for defamatory statements, and distributors were secondarily liable only under certain circumstances.[93] Court decisions established that conduits are not liable for the content they transmit,[94] that distributors are not liable for defamatory statements in the absence of knowledge of the defamatory statements,[95] and that distributors have no duty to monitor the content of publications.[96] Courts did not seem to agree on whether and how the rules should apply to Internet service providers; in one case a court held that a service provider was a distributor,[97] and in another,

90. Some have however, addressed this issue subsequently in slightly different ways. *See, e.g.,* the discussion of the EU E-Commerce Directive, *supra*.

91. *See* Stratton Oakmont v. Prodigy Servs. Co., 1995 N.Y. Misc. LEXIS 712 (N.Y. Sup. Ct. 1995).

92. 47 U.S.C. §230 (2006).

93. Felix T. Wu, *Collateral Censorship and the Limits of Intermediary Immunity*, 87 NOTRE DAME L. REV. 293, 310 (2011); *see also, e.g.,* Lerman v. Flynt Distributing Co, 745 F.2d 123 (2d Cir. 1984).

94. Wu, *supra* note 93, at 310; David S. Ardia, *Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity under Section 230 of the Communications Decency Act*, 43 LOY. L.A. L. REV. 373, 398–401 (2010).

95. RESTATEMENT (SECOND) OF TORTS § 581 (1965); Ardia, *supra* note 94, at 397, 398.

96. Lerman v. Flynt Distrib. Co., 745 F.2d 123, 139 (2d Cir. 1984).

97. Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135, (S.D.N.Y. 1991).

a court decided that a service provider was more a publisher than a distributor because of the content control that the service provider exerted.[98] The CDA responded to the court decisions by providing immunity from liability under defamation law and also under a wide variety of other laws.

The importance of Section 230 was quickly confirmed in case law. A key early case clarified that the CDA immunizes service providers from secondary liability, whether they act as publishers or distributors:

> By its plain language, § 230 creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service. Specifically, § 230 precludes courts from entertaining claims that would place a computer service provider in a publisher's role. Thus, lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions—such as deciding whether to publish, withdraw, postpone or alter content—are barred.[99]

The court in that case later explained that the reason this law was passed was to prevent a chilling of speech and because of the extreme burden that providers would face if this law had not been passed.[100] Notably, the court grounded its conclusion in part on the claim that the law promotes self-regulation.[101] Indeed, the Copyright Alert System described *infra* was negotiated in the shadow of Section 230, and adopted with the specific intent to shape a set of industry norms to the contours of the immunities provided by Section 230 as well as DMCA.[102]

Importantly, Section 230's coverage has been construed rather broadly. First, the immunity goes beyond traditional ISPs and additionally covers "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions."[103] Entities that have

98. Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995).

99. Zeran v. Am. Online, Inc., 129 F.3d 327, 330 (4th Cir., 1997).

100. *Id.* at 331.

101. *Id. See also* Doe v. Myspace, Inc, 474 F. Supp. 2d 843, 850 (W.D. Tex. 2007) ("This section reflects [. . .] the potential for liability attendant to implementing safety features and policies created a disincentive for [. . .] services to implement any safety features or policies at all").

102. Although Section 230 does not by its terms specify preemption of intellectual property infringement claims (such as copyright), and contains an IP savings clause in § 230(e)(2), it has been held to preempt federal intellectual property claims. Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102 (9th Cir. 2007).

103. 47 U.S.C. §230(f)(2) (2006).

benefited from this immunity include Facebook, Google and Yahoo! (as an email provider). Second, although it is often argued that Section 230 immunizes service providers only for actions in which they assume the role of a publisher or speaker, courts have applied the immunity even in cases where the service provider arguably did not act in that role.[104] Finally, Section 230 also immunizes service providers from civil liability that may be based on the provider's restricting access to certain types of material or on the provider's providing to others the technical means to restrict access to certain types of material.[105]

While the benefits of the CDA to ISPs and other providers of services on the Internet seem clear, there are costs, though these are not very visible. First, by providing immunity to service providers that merely convey others content, they have encouraged the spread and imitation of a particular form of Internet enterprise. There might be positives to Internet enterprises that both generated and published their own content with a higher degree of reliability, or that exercised more of a curatorial function over the content of others that they convey. However, Section 230 provides a relatively stark advantage to those Internet firms that hew to its conditions; all else being equal, this disadvantages the Internet enterprises that might have chosen a different tack. If new enterprises are influenced to choose structures that have already succeeded, that may bolster this effect. Second, and relatedly, by providing a clear roadmap for avoiding liability, the aid that Section 230 has given to the early development of Internet services may ironically be slowing its subsequent: immunity from civil liability comes at a cost to those whose otherwise valid claims are barred; to the extent that technological fixes might have avoided or reduced the harms that give rise to those claims, there is reduced incentive to develop such fixes in light of Section 230 immunity.

On balance, Section 230 is almost certainly a net positive over the history of the development of Internet services in the United States. However, going forward, there may be reason to ask whether its helping hand is turning into a crutch.

III. Self-Regulation: The New Copyright Alert System

The Copyright Alert System (CAS, also known as "six strikes") is an American attempt at implementing through private industry cooperation a "graduated response" system of the kind other nations have created through explicit legislation. While self-regulation may have important benefits, the creation of such a system without active participation by user representatives has drawn criticism. Indeed,

104. Doe v. MySpace, 528 F.3d 413 (5th Cir. 2008). *See also* Wu, *supra* note 93, at 327, 328.

105. 47 U.S.C. §230(c)(2) (2006).

the 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 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.

The CAS framework was implemented starting in February 2013, just six months prior to the time of this writing, and was devised through the negotiation and cooperation of several major industries and firms, notably the industry associations the 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; 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.

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.[106] 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. Certainly, the level of government involvement did not reach the level of formality—including statutory language—that has been seen in other nations that have adopted versions of graduated response (e.g., HADOPI in France). However, because the CAS was implemented through closed-door negotiations, some observers allege that the government may have been able to "cloak its own agenda" as part of a putatively private agreement.[107]

As a result of this development process, the CAS is built on a six-step process of notification to users. The first and second alerts notify ISP subscribers that their Internet account has allegedly been used for copyright infringement and provide an explanation of how to avoid future offenses. If the allegedly infringing behaviors continue, the third and fourth alerts are sent, and ask the subscriber to ac-

106. Timothy Lee, *What the 1930s Fashion Industry Tells Us About Big Content's "Six Strikes" Plan*, ARS TECHNICA (July 28, 2011), http://arstechnica.com/tech-policy/2011/07/what-the-1930s-fashion-industry-means-for-big-contents-six-strikes-plan.

107. Derek Bambauer, *The New American Way of Censorship,* 49-Mar. ARIZ. ATT'Y 32, 36 (2013).

knowledge their receipt. Should the behavior persist, a fifth alert is sent and ISPs are then allowed to take "mitigation measures" to stop further infringement. These mitigation measures include "temporary reductions of Internet speeds, redirection to a landing page until the subscriber contacts the ISP to discuss the matter or reviews and responses to some educational information about copyright, or other measures that the ISP may deem necessary."[108] 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.[109]

A major criticism of the CAS is that it represents private governance without the voice of the governed; some NGO groups, including the Electronic Frontier Foundation, have criticized the process that implemented and operates the CAS as lacking direct representation of user/consumer interests. While the CAS may evolve, by its structure and the nature of the industry players operating and participating in it, it is not likely to change in ways that directly reflect user demands. The governance structure of the CCI does not offer a strong role for user voices, and the monitoring of user activity for alleged infringement is outsourced to a private firm with little reason to provide avenues for users to voice challenges to the process or system. As a result, the industry players have effectively negotiated a joint constraint on user demands for change in the way alleged infringement is treated.

Another major concern with the CAS is that it tends to foreclose competition among ISPs over their policies balancing user rights with the concerns of copyright holders. In particular, an agreement among competing ISPs to effectively shift the burden of proof in infringement actions to the user effects a de facto significant change in users' substantive rights. Such an agreement benefits copyright holders at a cost to users, and it does so through competitors' collusion rather than by legislative action. To the extent that the CAS becomes an industry standard, it may effectively raise barriers against new en-

108. Center for Copyright Information FAQs, CENTER FOR COPYRIGHT INFORMATION, http://www.copyrightinformation.com/faq (last visited Sept. 25, 2013).

109. Annemarie Bridy, *Graduated Response American Style: Six Strikes Measured Against Five Norms,* 25 FORDHAM INTELL. PROP. MEDIA & ENT. L. J. 1 (2012).

trants seeking to provide Internet services. By including the copyright industry in the deal, it may have ensured that that industry's members will not license content to ISPs who do not adopt the new model.[110] As a result, the CAS may tend to form a barrier to entry, and possibly, to the innovation of insurgent firms.

CONCLUSION

The DMCA, the CDA and the CAS are not without their benefits. However, an under-appreciated aspect of these three regimes is the degree to which they may tend to benefit incumbent firms and ossify the development of Internet services. As a result, future policymaking should seek to avoid hindering technological development, and instead should create rules, standards and self-governance that incorporate dynamic change in its statutory language, institutions and application.

110. This may be a classic case of an arrangement in which vertical agreements are a means to help accomplish horizontal agreements' ends. *See, e.g.,* Fashion Originators' Guild of America v. FTC, 312 U.S. 457 (1938); United States v. Apple, No. 12 Civ. 2826(DLC), 2013 WL 4829312 (S.D.N.Y. 2013).