ANNEMARIE BRIDY*

Graduated Response and the Turn to Private Ordering in Online Copyright Enforcement

> Litigation is slow and the Internet is fast . . . . I don't think it makes much sense for us to ask the Government to be the police in this issue. What we would like is to be deputized to solve our own problems.[1]
>
> – Steven Soderbergh, Directors Guild of America

At the end of 2008, the Recording Industry Association of America (RIAA) concluded its five-year campaign of litigation against individual peer-to-peer (P2P) file sharers and announced that it would be shifting its online copyright enforcement efforts to a model known as graduated response.[2] As it has been presented by the RIAA and other industry groups, the enforcement paradigm embodied in graduated response eschews litigation and statutory mandates in favor of voluntary cooperation between rights owners and Internet access providers—parties that have long been at loggerheads with each other in the war on piracy. The Business Software Alliance (BSA), for example, has publicly advocated bypassing Congress to

* Associate Professor of Law, University of Idaho College of Law. The author would like to thank Casey Inge, Lydia Pallas Loren, David Post, Peter Yu, and the participants in the 2010 Intellectual Property Scholars Roundtable at Drake University School of Law for their valuable feedback.

1 *Sinking the Copyright Pirates: Global Protection of Intellectual Property: Hearing Before the H. Comm. on Foreign Affairs*, 111th Cong. 28 (2009) (statement of Steven Soderbergh, National Vice President, Directors Guild of America), *available at* http://foreignaffairs.house.gov/111/48986.pdf.

2 Sarah McBride & Ethan Smith, *Music Industry to Abandon Mass Suits*, WALL ST. J., Dec. 19, 2008, at B1, *available at* http://online.wsj.com/article/SB122966038836021137.html.

pursue a "voluntary industry-led approach," which it predicts will prove more effective than further governmental intervention along the lines of the Digital Millennium Copyright Act (DMCA).[3] A representative of the RIAA expressed the same view in testimony before Congress concerning the proposed Internet Freedom and Preservation Act of 2008.[4] More recently, in comments filed with the Federal Communications Commission (FCC) in connection with the notice of proposed rule-making concerning the preservation of the open Internet (the Open Internet NPRM), the Motion Picture Association of America (MPAA) asked the government to step aside and "not interpose any legal or regulatory obstacles" (e.g., in the form of net neutrality mandates) that would prevent rights owners and broadband providers from working together to implement graduated response.[5] Unlike in Europe and other places abroad, where trade associations representing corporate rights owners have advocated with some success for legislatively mandated graduated response regimes, the domestic campaign—so far, at least—has focused on interindustry negotiations involving technology-based solutions capable of private implementation.[6]

---

[3] *BSA Position on Appropriate Measures to Deter Online Piracy of Content*, BUSINESS SOFTWARE ALLIANCE, http://www.bsa.org/country/Public%20Policy/online-content-piracy.aspx (last visited Oct. 2, 2010).

[4] *The Internet Freedom Preservation Act of 2008: Hearing on H.R. 5353 Before the H. Subcomm. on Telecomms. and the Internet of the H. Comm. on Energy and Commerce*, 110th Cong. (2008) (written statement of Mitch Bainwol, Chairman and CEO, RIAA), *available at* http://76.74.24.142/F382DD78-ECE4-2026-BD0C-33C4ED1A0D44.pdf ("Our view is that the marketplace is generally a better mechanism than regulation for addressing such complex issues as how to address online piracy."); Recording Indus. Ass'n of Am., *RIAA CEO Encourages ISPs to Work with Music Industry to Address Digital Theft*, RIAA NEWS ROOM (May 6, 2008), http://www.riaa.com/newsitem.php?news_month_filter=5&news_year_filter=2008&resultpage=2&id=445DBB88-3C46-F2B7-784F-8B1B1B7F5FAA (announcing "constructive discussions with a number of ISPs about ways to address the piracy problem, including mechanisms like graduated response . . . and business solutions through negotiations between individual music companies and ISPs that can capture the value of music being consumed by subscribers").

[5] *In the Matter of A National Broadband Plan For Our Future: Comments of the Motion Picture Ass'n of Am., Inc. in Response to the Workshop on the Role of Content in the Broadband Ecosystem Before the Fed. Commc'ns Comm'n*, GN Docket No. 09-51, at 21 (2009), *available at* http://www.mpaa.org/Resources/b55c4e2c-3510-424d-b12f-6719b86552ea.pdf.

[6] For a full discussion of the efforts that have been and are being made abroad, including the highly controversial adoption of a mandatory three-strikes regime in France, see Jeremy de Beer & Christopher D. Clemmer, *Global Trends in Online Copyright Enforcement: A Non-Neutral Role for Network Intermediaries?*, 49 JURIMETRICS J. 375 (2009). With respect to domestic strategy, Cary Sherman, the RIAA's President, has stated that there is no need to "relegislate" the role of ISPs in enforcing copyrights online,

This turn to private ordering and technology-based solutions represents a departure from the dominant strategies of lobbying and litigation that corporate rights owners have pursued domestically since the early days of the digital revolution. On the lobbying front, rights owners pressed for—and won—greater statutory protection of copyrights and stiffer penalties for infringement.[7] On the litigation front, they sued—and beat—both the purveyors and the users of disruptive technologies for copying and distributing digital content, most notably P2P software.[8] None of these efforts, however, made much of a dent in the prodigious volume of illegally traded files.[9] Hence, the emerging belief among rights owners is that the time is ripe for a strategic shift away from public law and litigation,[10] toward partnerships with internet service providers (ISPs)[11] and an

and the RIAA is "much more interested in finding a marketplace way of going about this." Anne Broache, *RIAA: No Need to Force ISPs by Law to Monitor Piracy*, CNET NEWS, Jan. 30, 2008, http://news.cnet.com/8301-10784_3-9861460-7.html (quoting Cary Sherman). Sherman acknowledged that the approach being taken abroad, particularly in Europe, is "more of a regulatory approach." *Id.*

7 These include, for example, the anti-circumvention provisions of the Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified in scattered sections of 17 U.S.C.), the redefinition of criminal infringement and its penalties in the No Electronic Theft (NET) Act, Pub. L. No. 105-147, 111 Stat. 2678 (1997), and the extension of the term of copyright in the Sonny Bono Copyright Term Extension Act, Pub. L. No. 105-298, 112 Stat. 2827 (1998).

8 *See generally* Annemarie Bridy, *Why Pirates (Still) Won't Behave: Regulating P2P in the Decade After Napster*, 40 RUTGERS L.J. 565 (2009) (discussing the leading cases against both P2P software providers and individual file sharers).

9 According to the International Federation of the Phonographic Industry (IFPI), which represents music industry trade associations worldwide and which collated studies from sixteen countries over a four-year period, an estimated forty billion music files were illegally shared in 2008, which represents ninety-five percent of all downloaded music. IFPI, DIGITAL MUSIC REPORT 2009: NEW BUSINESS MODELS FOR A CHANGING ENVIRONMENT 22 (2009), *available at* http://www.ifpi.org/content/library/DMR2009-real.pdf. There is, however, justified skepticism concerning industry-generated statistics relating to online piracy and piracy-related economic losses. *See, e.g.*, Nate Anderson, *Rep "Hollywood" Berman Calls for New IP Law—Using Dodgy Data*, ARS TECHNICA, Apr. 8, 2009, http://arstechnica.com/tech-policy/news/2009/04/rep-howard-berman-calls-for-new-ip-law-using-dodgy-data.ars (pointing out that the IFPI also found, but did not emphasize, that only eighteen percent of Internet users in Europe actually share files illegally).

10 Peter Yu has pointed out the ways in which "the graduated response system provides an attractive alternative to many of the unpopular legal tactics deployed via civil lawsuits and criminal prosecutions." Peter Yu, *The Graduated Response*, 62 FLA. L. REV. (forthcoming 2010).

11 The term "ISP" is often used broadly to encompass both Internet access providers and other types of online service providers; however, I use it throughout this Article

enforcement regime that operates on Internet users through a combination of technology and private law mechanisms, such as standardized terms of service and acceptable use policies.[12]

The most widely publicized form of graduated response is a "three strikes and you're out" model, in which Internet access is suspended or terminated by a user's ISP following the user's receipt of three successive notices of copyright infringement.[13] The division of labor between rights owners and ISPs with respect to monitoring and notification of infringement varies from one permutation of graduated response to the next. The most aggressive and controversial regime, for example, is one in which ISPs implement filtering technologies within their networks and fully automate the processes of notification and termination/suspension.[14] Some colleges and universities have already adopted this model of graduated response in an effort to comply with the Higher Education Opportunity Act of 2008 (HEOA), which expressly requires them to develop copyright enforcement plans that include technology-based deterrents to online infringement.[15] Regardless of the precise division of labor, in all

exclusively to denote Internet access providers, most of which are now providers of broadband access.

12 Music industry representatives have emphasized publicly, however, that if voluntary agreements with ISPs cannot be reached, they will pursue legislation mandating cooperation. *See* Declan McCullagh, *Music, Movie Lobbyists Push to Spy on Your Net Traffic*, CNET NEWS, Aug. 18, 2008, http://news.cnet.com/8301-13578_3-10019622-38.html ("A representative of the recording industry said . . . that her companies would prefer to enter into voluntary 'partnerships' with Internet service providers, but pointedly noted that some governments are mandating such surveillance 'if you don't work something out.'"); Recording Indus. Ass'n of Am., *supra* note 4 (asserting that "government action may be necessary" if ISPs do not embrace a marketplace solution).

13 This model has been advocated publicly by the Business Software Alliance (BSA), a trade group representing software manufacturers. *See* BUSINESS SOFTWARE ALLIANCE, *supra* note 3. The BSA favors the use of "[a]utomated educational notification mechanisms for alleged online infringers" and "[t]he imposition of appropriate sanctions, including . . . the suspension or termination of Internet service for individual repeat offenders." *Id.* The RIAA has been actively pursuing graduated response agreements with ISPs. *See* McBride & Smith, *supra* note 2 (reporting on preliminary deals with ISPs pursuant to which repeat notifications of infringement are to be followed by termination of access).

14 This comprehensive and fully automated form of graduated response is offered by Audible Magic, among others. Audible Magic offers an appliance called CopySense, which is widely marketed to IT departments at colleges and universities. *Solutions for Colleges & Universities*, AUDIBLE MAGIC, http://www.audiblemagic.com/solutions/universities.asp (last visited Oct. 2, 2010).

15 The HEOA conditions participation in federal financial aid programs on certification that the participating institution "has developed plans to effectively combat the unauthorized distribution of copyrighted material, including through the use of a variety of

forms of graduated response the onus of enforcing digital copyrights is shared between content providers and ISPs, and repeated notices of infringement—from whichever source they emanate—culminate in at least a temporary suspension of Internet access.[16]

This Article seeks to explain why voluntary graduated response, as publicly controversial as it is, is squarely on the table as corporate rights owners and broadband providers discuss their respective roles in the future of online copyright enforcement.[17] It situates the rapprochement now taking place between the two groups within the context of copyright law's special rules of liability for intermediaries that act as "mere conduits" for their customers' communications. These rules, which have historically insulated ISPs from liability for the infringing transmissions of their customers, are becoming less clearly applicable as broadband providers deploy "intelligent" routers within their networks, giving them the ability to inspect, sort, and filter the traffic they carry.[18] As broadband business models evolve away from the traditional model of passive carriage, ISPs risk sacrificing the special protections that have developed over time to shield neutral intermediaries from liability for copyright infringement. This potential exposure gives ISPs a compelling incentive to explore private partnerships with rights owners that would once have been politically unthinkable.

technology-based deterrents." 20 U.S.C.S. § 1094(a)(29)(A) (LexisNexis 2009). Rules promulgated under the HEOA require that these plans be implemented effective July 1, 2010. *See* 34 C.F.R. § 668.14 (2010). According to Audible Magic's Web site, the CopySense appliance is in use at over fifty colleges and universities. *See CopySense Customers—Colleges & Universities*, AUDIBLE MAGIC, http://www.audiblemagic.com/clients-partners/copysense.asp (last visited Oct. 2, 2010).

16 The IFPI couches discussions of graduated response in terms of "extending responsibility for copyright protection across the value chain to include ISPs." IFPI, *supra* note 9, at 24.

17 High-level representatives from both camps have come together publicly in venues such as the Progress and Freedom Foundation's Aspen Summit in 2008 and the Leadership Music Digital Summit in 2009. *See* Chloe Albanesius, *Comcast, Others Deny 'Three Strikes' Piracy Plan*, PCMAG.COM, Mar. 27, 2009, http://www.pcmag.com/article2/0,2817,2343977,00.asp (reporting on the Leadership Music Digital Summit); McCullagh, *supra* note 12 (reporting on the Aspen Summit).

18 *See* Rob Frieden, *Internet Packet Sniffing and Its Impact on the Network Neutrality Debate and the Balance of Power Between Intellectual Property Creators and Consumers*, 18 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 633, 645 (2008) ("The output of affordable deep packet inspection and other technologies now available to ISPs raises questions whether non-neutral network operation disqualifies ISPs for a safe harbor exemption from liability for carrying copyright infringing traffic provided by § 512 of the DMCA.").

Part I of this Article examines the treatment of so-called conduit ISPs under the safe harbor framework of the DMCA. It focuses on the interaction between § 512(a), which governs providers of routing, transmission, and connection services, and two other provisions of the DMCA—§ 512(i), which concerns the punishment of repeat infringers, and § 512(h), which concerns the issuance of subpoenas to identify alleged infringers. Section 512(i) and the cases interpreting it provide a credible rationale for ISP adoption of graduated response that predates both the use of the catchphrase and the attention the concept has lately attracted in the tech media.[19] Section 512(h) and the cases interpreting it are relatively less helpful to rights owners vis-à-vis conduit ISPs, but they have prompted the negotiation of private agreements pursuant to which major ISPs voluntarily forward notices of infringement to customers. These limited agreements, which are in the spirit of cooperation that the DMCA was intended to foster, may represent the first step in a more complete private ordering of the project of online copyright enforcement.

Part II of this Article explores the liability implications of departing, as broadband ISPs have, from the model of passive carriage contemplated in § 512(a). It begins with an abridged history of common carriage, goes on to consider copyright liability rules (other than the DMCA) that ease burdens on passive carriers, and concludes with a discussion of the legal consequences that may flow from the decision of broadband providers to implement intelligent network technology to gain greater control over the traffic that crosses their networks. Considering these consequences, it may be no more than prudent from a liability standpoint for broadband operators to engage with content owners in a renegotiation of the division of labor for online copyright enforcement.

Part III concerns the potential impact of such a renegotiation on broadband users, who have come to rely on uninterrupted Internet connectivity to participate in an ever-widening range of important life activities that are unrelated to commerce in copyrighted digital works. Proceeding from the premise that the government is unlikely in the name of net neutrality to prohibit ISPs from blocking infringing file transfers, Part III proposes a number of principles to guide private

[19] Coverage of graduated response in the tech media tends to elide the fact that the DMCA, now over ten years old, contains a provision—section 512(i)—that contemplates the termination of service for repeat copyright infringers. *See, e.g.*, Greg Sandoval, *AT&T First to Test RIAA Antipiracy Plan*, CNET NEWS, Mar. 24, 2009, http://news.cnet.com/8301-1023_3-10203799-93.html.

ordering in the arena of online copyright enforcement so that consumers do not become victims of immature filtering technologies and overzealous enforcement.

I
"CONDUIT" ISPS, THE DMCA, AND THE WAR ON P2P

A. A Refuge for Passive Carriers: § 512(a)

When it comes to liability for online copyright infringement, the safe harbor provisions in § 512 of the DMCA have defined the legal environment for ISPs for more than a decade.[20] It's worth bearing in mind, however, that it was once far from given that online service providers should be in any way relieved of liability for the infringements of their customers or that they should not be required to take costly steps to police their networks for infringing content transmitted or stored by their customers.[21] Indeed, if Congress had been persuaded in 1995 by the recommendations of President Clinton's Information Infrastructure Task Force (IITF), ISPs would have been pressed into service as active copyright enforcers long ago through the operation of liability rules developed in and for the analog age.[22]

In its much anticipated 1995 report on the National Information Infrastructure, now known simply as the "White Paper," the IITF rejected arguments that the growth of the Internet and the viability of online services would be threatened by liability rules under which providers would be responsible for the copyright infringements of their subscribers.[23] The IITF saw a number of reasons, both pragmatic and philosophical, for not letting ISPs off the hook for the infringing activities of their subscribers. One was that ISPs are well positioned to serve an enforcement function because they have the

20 *See* 17 U.S.C. § 512 (2006).

21 *See, e.g.*, Playboy Enters., Inc. v. Frena, 839 F. Supp. 1552, 1556 (M.D. Fla. 1993) (holding the operator of a BBS liable for copyright infringement because he "supplied a product containing unauthorized copies," even though he himself did not make the copies of the infringing pictures).

22 *See* BRUCE A. LEHMAN, U.S. PATENT AND TRADEMARK OFFICE, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE: THE REPORT OF THE WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS 114–24 (1995), *available at* http://www.uspto.gov/web/offices/com/doc/ipnii/ipnii.pdf (making recommendations concerning the scope of online service provider liability for copyright infringement).

23 *Id.* at 115–17.

ability to disconnect subscribers who break the law.[24] Another was that immunity could give providers a perverse incentive to remain willfully ignorant of illegal activity occurring on their systems.[25] A third was that ISPs "reap rewards for infringing activity" in the form of added subscribers and increased usage, and they should therefore "bear the responsibilities" associated with that activity.[26] Given all of these factors, the IITF concluded that liability for distributing illegal content provided by others is rightly treated as a cost of doing business for all information distributors, regardless of whether they do business in real space or cyberspace.[27] To alter existing standards of liability in any way, the IITF said, "would result in a substantial derogation of the rights of copyright owners."[28] In the proposed legislation submitted with the White Paper, there were thus no provisions that would in any way have insulated or protected online intermediaries from liability arising from their users' infringing conduct.[29]

Although the IITF thought it was "premature to reduce the liability of any type of service provider,"[30] it did recognize that a one-size-fits-all approach might not be the best policy, given the diverse functions that online providers serve:

> On-line service providers currently provide a number of services. With respect to the allowance of uploading of material by their subscribers, they are, in essence, acting as an electronic publisher. In other instances, they perform other functions. No one rule may be appropriate. If an entity provided only the wires and conduits—such as the telephone company, it would have a good argument for an exemption if it was truly in the same position as a common carrier and could not control who or what was on its system. The same could be true for an on-line service provider who unknowingly transmitted encrypted infringing material.[31]

[24] *Id.* at 122–23.

[25] *Id.* at 122.

[26] *Id.* at 117–18.

[27] *Id.* at 117 (pointing out that "this problem has been a part of the cost of doing business for many other distributors of material that is provided to them by others"); *id.* at 118 (stating, again, that "[t]he risk of infringement liability is a legitimate cost of engaging in a business that causes harm to others").

[28] *Id.* at 114.

[29] *See id.* at app. 1.

[30] *Id.* at 122.

[31] *Id.*

As we know from the subsequent passage of the DMCA, which contains safe harbors for providers of four[32] discrete types of online activities, Congress did not follow the IITF's recommendation to leave online service providers fully exposed to liability for the copyright infringements of their subscribers. Congress did, however, incorporate into the structure of the DMCA's safe harbors the significant distinction the IITF saw between online service providers that *store* material uploaded by users and those that merely *route and transmit* material for users.[33] Consistent with the IITF's logic concerning which of the two types of providers is better situated to know and control what its subscribers are doing, Congress required more in the way of compliance under § 512 from providers acting like information publishers than it did from providers acting like information conduits.[34] Providers that act more like publishers—those that store information in a persistent way at the direction of users—are subject to the "notice and takedown" regime set forth in § 512(c) of the DMCA.[35] By contrast, providers that act more like conduits or common carriers—those that route and transmit information without modifying it or storing it more than fleetingly—are governed by § 512(a), which does not predicate eligibility for the safe harbor on compliance with § 512(c)'s notice and takedown regime.[36]

32 17 U.S.C. § 512(a) (2006) (governing transitory digital network communications); *id.* § 512(b) (governing system caching); *id.* § 512(c) (governing information residing on systems or networks at the direction of users); *id.* § 512(d) (governing information location tools).

33 *See id.* § 512(a) (governing transitory digital network communications); *id.* § 512(c) (governing information residing on systems or networks at direction of users).

34 *Compare id.* § 512(a) *with id.* § 512(c). *See also* Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Servs., Inc., 351 F.3d 1229, 1234 (D.C. Cir. 2003) ("Notably present in §§ 512(b)–(d), and notably absent from § 512(a), is the so-called notice and take-down provision.").

35 *See* 17 U.S.C. § 512(c)(1)(A).

36 *See id.* § 512(a); *In re* Charter Commc'ns, Inc., 393 F.3d 771, 776 (8th Cir. 2005) (noting that Section 512(a) does not require compliance with the DMCA's notice and takedown provisions); Io Grp., Inc. v. Veoh Networks, Inc., 586 F. Supp. 2d 1132, 1147 (N.D. Cal. 2008) (explaining that "[t]he statute itself is structured in a way that distinguishes between so-called 'conduit only' functions under Section 512(a) and those functions addressed by Section 512(c) (and other subsections as well)").

B. Obligations of Conduit Providers: § 512(a) and (i)

Further differentiating "conduit" service providers from other service providers eligible under § 512's safe harbors, Congress specifically defined § 512(a) providers in § 512(k):

> As used in subsection (a), the term "service provider" means an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received.[37]

In order for an ISP that meets the definition in § 512(k) to come within the protection of the safe harbor in § 512(a), five conditions must be met, all of which have to do with the ISP's functioning like a common carrier—providing, in the words of the IITF, "only the wires and conduits"[38] through which someone else's information travels: (1) the transmission must be initiated by someone other than the provider; (2) the transmission must be "carried out through an automatic technical process without selection of the material by the service provider;" (3) the provider must not select the recipient of the transmission; (4) the provider must not maintain a copy of the material on its system for longer than is necessary to transmit it; and (5) the material must be transmitted "without modification of its content."[39]

Although conduit ISPs that fall within the scope of § 512(a)'s protections for providers of transitory digital network communications are not required to comply with the DMCA's notice and takedown framework, all defendants seeking safe harbor under § 512 are subject to conditions for eligibility set forth in § 512(i).[40] Section 512(i) requires service providers to (1) adopt a policy that provides for the termination of access for repeat infringers in appropriate circumstances, (2) implement that policy in a reasonable manner, and (3) inform its subscribers of the policy.[41] It also requires service providers to accommodate and "not interfere with standard

---

[37] 17 U.S.C. § 512(k)(1)(A).

[38] LEHMAN, *supra* note 22, at 122.

[39] 17 U.S.C. § 512(a)(1)–(5).

[40] Perfect 10, Inc. v. CCBill LLC, 481 F.3d 751, 758 (9th Cir. 2007) (stating that "[t]o be eligible for any of the four safe harbors at §§ 512(a)–(d), a service provider must first meet the threshold conditions set out in § 512(i)").

[41] 17 U.S.C. § 512(i)(1)(A); Ellison v. Robertson, 357 F.3d 1072, 1080 (9th Cir. 2004).

technical measures" used by copyright owners to identify and protect their works.[42]

Compared to the detailed notice and takedown framework from § 512(c), the requirements of § 512(i) are much more loosely defined. For example, the statute provides no definition of "repeat infringer" and is silent as to what "appropriate circumstances" for termination of access might be.[43] The statute does not define what it means for a policy to be "reasonably implemented," nor does it specify the means by which an ISP is expected to "inform subscribers" of its policy. As one court has observed, "the language of the statute and the legislative history of this section are less than models of clarity."[44] Courts asked to decide copyright infringement claims in which defendant ISPs have asserted one or more of the § 512 safe harbors have thus been forced as a matter of statutory construction to give more definite content to § 512(i) than Congress did when it drafted the DMCA. In doing so, they have been guided by a legislative history expressing Congressional intent to preserve strong incentives for service providers to cooperate with rights owners.[45] At the same time, however, they are bound to interpret § 512(i)'s requirements within the limits of § 512(m), the DMCA's privacy provision, which expressly precludes courts from construing any provision in § 512 to condition safe harbor eligibility on "a service provider monitoring its service or affirmatively seeking facts indicating infringing activity."[46] So, while § 512(i) was designed to promote cooperation between rights owners and ISPs in online copyright enforcement, it cannot be

42 17 U.S.C. § 512(i)(1)(B).

43 *See generally* Andres Sawicki, *Repeat Infringement in the Digital Millennium Copyright Act*, 73 U. CHI. L. REV. 1455 (2006). In *UMG Recordings, Inc. v. Veoh Networks Inc.*, the court declined to hold that termination of a user's access was required after a second notice when the first notice identified multiple alleged infringements. UMG Recordings, Inc. v. Veoh Networks Inc., 665 F. Supp. 2d 1099, 1118 (C.D. Cal. 2009). The notices in the case were generated by the copyright owner using Audible Magic's filtering system. *Id.*

44 Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1176 (C.D. Cal. 2002).

45 *See In re* Charter Commc'ns, Inc., 393 F.3d 771, 782 (8th Cir. 2005) (quoting the legislative history of the DMCA to establish that "Congress wanted to create 'strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment'" (quoting S. REP. NO. 105-190, at 40 (1998))).

46 17 U.S.C. § 512(m)(1).

read in light of § 512(m) to impose on qualifying ISPs any affirmative duty to monitor or investigate.[47]

An additional limitation on what can be required of qualifying providers under § 512(i) is the DMCA's narrow definition of the types of standard technical measures that providers must accommodate in order to qualify for safe harbor.[48] Such measures must "have been developed pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process;"[49] they must be "available to any person on reasonable and nondiscriminatory terms;"[50] and they must "not impose substantial costs on service providers or substantial burdens on their systems or networks."[51] Perhaps because the incentives of the parties whose consensus is required have historically been misaligned, the standard technical measures provision of § 512(i) has not yet resulted in any concrete obligations for providers—although this may now be changing for reasons that are discussed at length in Part II of this Article.[52]

Given the express limitation established in § 512(m) concerning the burdens and costs that can legitimately be imposed on providers seeking safe harbor, courts have produced carefully calibrated interpretations of the reach of § 512(i), most in the context of defenses raised under § 512(c). For example, in *Corbis Corp. v. Amazon.com, Inc.*,[53] the court held that a properly adopted termination policy need not precisely track the language of the DMCA, and it need not disclose to users the precise criteria the provider will apply to determine when termination of access is appropriate.[54] Such a policy must, however, convey to users "who repeatedly or flagrantly abuse their access to the [I]nternet through disrespect for the intellectual property rights of others" that they face

47 *See, e.g.*, Io Grp., Inc. v. Veoh Networks, Inc., 586 F. Supp. 2d 1132, 1145 (N.D. Cal. 2008) (stating that "section 512(i) does not require service providers to track users in a particular way or to affirmatively police users for evidence of repeat infringement").

48 *See* 17 U.S.C. § 512(i)(2) (defining "standard technical measures").

49 *Id.* § 512(i)(2)(A).

50 *Id.* § 512(i)(2)(B).

51 *Id.* § 512(i)(2)(C).

52 *See* 3 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 12B.02[B][3] (2006) (expressing doubt that the provision will ever lead to concrete obligations, given the incentives of the parties).

53 Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090 (W.D. Wash. 2004).

54 *Id.* at 1101–02.

"a realistic threat of losing that access."[55] In *Perfect 10, Inc. v. Cybernet Ventures, Inc.*,[56] the court held that determining appropriate circumstances for termination does not require investigation by the provider into individual acts of infringement; however, the provider must act when it receives "sufficient evidence to create actual knowledge of blatant, repeat infringement by particular users, particularly infringement of a willful and commercial nature."[57]

Courts have not spoken with one voice when it comes to what and how much § 512(i) specifically requires of safe-harbor-seeking providers. While courts seem to agree that § 512(i) requires providers to have in place a system for receiving notices of infringement from rights owners,[58] they have reached differing conclusions concerning whether multiple notices of infringement from a copyright owner are sufficient, on their own, to justify charging a provider with actual knowledge of a particular user's blatant, repeat infringement.[59] And some courts have held that something less than actual knowledge of blatant infringement can establish circumstances requiring termination under § 512(i) because § 512(i) should be read to incorporate § 512(c)'s "red flag" test.[60] Under the red flag test, a service provider may lose safe harbor if it fails to act when it is "aware of facts or circumstances from which infringing activity is

[55] *Id.* at 1101 (quoting H.R. REP. NO. 105-551, pt. 2, at 44 (1998)).

[56] Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146 (C.D. Cal. 2002).

[57] *Id.* at 1177.

[58] *See, e.g.*, Perfect 10, Inc. v. CCBill LLC, 481 F.3d 751, 758 (9th Cir. 2007) (holding that § 512(i) requires "a working notification system"); Ellison v. Robertson, 357 F.3d 1072, 1080 (9th Cir. 2004) (holding that a reasonable jury could conclude that implementation of a termination policy is not reasonable where notices of infringement have gone unheeded by the provider); *Corbis Corp.*, 351 F. Supp. 2d at 1102 (holding that § 512(i) requires adoption and implementation of a procedure for receiving complaints and conveying them to users).

[59] *Compare* Perfect 10, Inc. v. CCBill, LLC, 340 F. Supp. 2d 1077, 1088 (C.D. Cal. 2004) (concluding that "an internet service provider who receives repeat notifications that substantially comply with the requirements of § 512(c)(3)(A) about one of its clients, but does not terminate its relationship with the client, has not reasonably implemented a repeat infringer policy"), *rev'd on other grounds*, 481 F.3d 751, *with Corbis Corp.*, 351 F. Supp. 2d at 1105 (concluding that notices from a copyright owner function to bring a potential infringement to the provider's attention, but do not, in themselves, provide evidence of blatant copyright infringement because they could be erroneous).

[60] *See* CCBill LLC, 481 F.3d at 763; Arista Records LLC v. Usenet.com, Inc., 633 F. Supp. 2d 124, 142 (S.D.N.Y. 2009).

apparent"[61] (i.e., when it has constructive knowledge of infringement).

Because all providers seeking safe harbor under § 512 are subject to § 512(i), the incorporation of the notice and red flag provisions from § 512(c) into § 512(i) seems to implicate providers invoking § 512(a), even though it is clear on the face of the statute that they are not subject to the notice and takedown regime in § 512(c). Reading § 512(i) in a way that effectively makes elements of § 512(c) binding on all providers seeking safe harbor, including those invoking § 512(a), undermines the DMCA's scheme for imposing different and less onerous conditions for eligibility under § 512(a) (i.e., for conduit providers) than are imposed under § 512(b), (c), and (d), all of which expressly require compliance with the notice and takedown regime.[62] Moreover, such a reading is at odds with the established canon of construction that the meaning of individual statutory provisions should be interpreted in light of the statute as a whole.[63]

Taking into account the language of § 512(a), (i), (k), and (m) and the court decisions interpreting § 512(i) to incorporate elements from § 512(c), the requirements that must be met by an ISP seeking safe harbor under § 512(a) can be summarized as follows: First, the ISP must function solely as a conduit for the data communications of its users, in the same way that phone companies acting as common carriers historically functioned with respect to the voice communications of their users. In other words, it cannot select the material it transmits or in any way modify the content of that material. Second, it must comply with the requirements of § 512(i) concerning the termination of repeat infringers and accommodation of standard technical measures. Under the reading of § 512(i) that incorporates the "red flag" provisions from § 512(c), a provider invoking § 512(a) that actually knows or should know of blatant, repeat infringement by a particular user (i.e., "appropriate circumstances") must terminate the access of that user in order to show that it has "reasonably implemented" its repeat infringer policy. Finally, although the provider is not required to investigate or monitor its service to identify repeat infringers, it is required to have a process in place for

61 17 U.S.C. § 512(c)(1)(A)(ii) (2006).

62 *See id.* § 512(b)(2)(E), (d)(3) (conditioning eligibility on compliance with § 512(c)(3)).

63 K Mart Corp. v. Cartier, Inc., 486 U.S. 281, 291 (1988) ("In ascertaining the plain meaning of the statute, the court must look to the particular statutory language at issue, as well as the language and design of the statute as a whole.").

receiving and conveying to users notices of infringement sent by rights owners.

C. Conduit Providers, Repeat Infringers, and Graduated Response

Because the case law is mixed on the very important question of whether notices from rights owners, by themselves, can create requisite knowledge for the provider that a particular user is a repeat infringer, the most conservative course of action for a provider invoking § 512(a) is to terminate access for any user who is the subject of multiple notices of infringement from a copyright owner. This is, as it happens, consistent with the "three strikes" permutation of graduated response described in the opening paragraph above. In this particular division of labor, monitoring and notification are carried out by the copyright owner, and the sanction is imposed by the ISP at the behest of the copyright owner. From the provider's point of view, terminating any customer's access is a distasteful prospect because every user's continued access translates into revenue for the provider and users whose access is terminated can usually take their business to a competitor. From the user's point of view, termination at the behest of an aggrieved rights owner or owners without any neutral adjudication of the merits of the claims seems biased and unfair. It creates the impression that the provider has been co-opted by rights owners whose interests appear to be more important than the interests of the ISP's own customers.

The interpretation of § 512(i) that equates receipt of repeat notices of infringement with knowledge by the ISP that its user is a repeat infringer allows the copyright owner to be judge and jury for purposes of determining whose access the ISP must terminate in order to stay within the safe harbor. In effect, this reading of § 512(i) makes compliance with a "three strikes and you're out" form of graduated response, or something very like it, a precondition for safe harbor eligibility under § 512(a). The provider finds itself caught between Scylla and Charybdis: if it fails to terminate a user's access after receiving repeat notices of infringement from a copyright owner, it faces the loss of the safe harbor for not having reasonably implemented its termination policy; if, on the other hand, it terminates a user's access on the copyright owner's say-so, it faces the loss of a customer, which is especially troubling if the claims of infringement turn out to be misdirected or non-meritorious. Moreover, wrongful

terminations might themselves create the potential for provider liability to customers for breach of contract.

The DMCA, which was drafted with the stated purpose of balancing the interests of rights owners and online providers, should not be read to put the provider in such a bind. The judicial interpretation of § 512(i) that better preserves the policy balance struck by Congress when it adopted the DMCA is one that requires something more than notices of infringement generated by rights owners before the provider can be charged with knowledge that a particular user is a repeat infringer.[64] Such additional evidence should be required especially when it comes to § 512(a) ISPs, which by definition lack knowledge of what is passing through their networks at any given time. Because § 512(a) providers are in less of a position to know what their users are transmitting than § 512(c) providers are to know what they are storing on behalf of their users, knowledge should not as readily be imputed to § 512(a) providers. Even the IITF, which opposed any limitation of liability for ISPs, appreciated that the two types of providers are on a different footing in terms of their relationships to their customers' data. Interpreting § 512(i) to impose § 512(c)'s notice and "red flag" elements on § 512(a) providers ignores the architecture of the DMCA and collapses definitional distinctions between the two types of providers that are plain on the statute's face.

D. Conduit Providers, P2P Architecture, and the Limits of the DMCA

The fact that elements from § 512(c), which governs the storage of user-supplied information, figure so prominently in judicial interpretations of § 512(i), which also governs conduit ISPs, is symptomatic of the DMCA's underlying assumption of a specific technological state of the art.[65] The statute was designed, as Niva Elkin-Koren and others have observed, to address a centralized network architecture in which communication among users is

[64] *See Corbis Corp.*, 351 F. Supp. 2d at 1105–06; UMG Recordings, Inc. v. Veoh Networks Inc., 665 F. Supp. 2d 1099, 1118 (C.D. Cal. 2009).

[65] Niva Elkin-Koren, *Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic*, 9 N.Y.U. J. LEGIS. & PUB. POL'Y 15, 41 (2006); *see also* Mike Scott, *Safe Harbors Under the Digital Millennium Copyright Act*, 9 N.Y.U. J. LEGIS. & PUB. POL'Y 99, 137 (2006) (arguing that "the statute . . . embodies particular normative and descriptive notions about how digital networks should work, as well as how they actually do work").

mediated by the ISP acting as a host for uploaded files.[66] Before the advent of P2P file sharing, storage on behalf of users—the function covered by § 512(c)—was the most copyright-relevant function an ISP performed. In P2P networks, however, files exchanged between users are never uploaded to an ISP's server; instead, they remain at all times on the users' own computers, from which they are directly copied by other users.[67] In this architecture, the most copyright-relevant functions an ISP performs are routing and transmission—the functions covered by § 512(a). Because the DMCA was designed primarily to deal with ISPs serving a centralized file storage function, it has proven to be a poor fit in cases involving P2P, where the ISP functions only as a conduit for the transfer of infringing material. This poor fit is perhaps best exemplified in the cases involving § 512(h), the DMCA's expedited subpoena provision, which rights owners sought to use at the peak of the file sharing phenomenon to compel conduit ISPs to reveal the identities of allegedly infringing users of P2P software.[68]

Section 512(h) permits a copyright owner to obtain a subpoena outside the context of litigation to identify an alleged infringer.[69] In order for the subpoena to issue, the copyright owner must submit to the clerk of the court a request consisting of three documents: a copy of the notification described in § 512(c)(3)(A); a proposed subpoena; and a sworn declaration that the subpoena is being sought "to obtain the identity of an alleged infringer and that such information will only be used for the purpose of protecting" a copyright.[70] The notification described in § 512(c)(3)(A), in order to be compliant with the statute's requirements, must identify, among other things, "the material that is claimed to be infringing . . . and that is to be removed or access to which is to be disabled" by the ISP.[71]

---

66 *See* Elkin-Koren, *supra* note 65, at 41; *see also* Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Servs., Inc., 351 F.3d 1229, 1238 (D.C. Cir. 2003) (referring to the establishment of "unauthorized FTP or BBS sites on the servers of ISPs").

67 *See generally* A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1011 (9th Cir. 2001) (explaining how a P2P system works).

68 *See In re* Charter Commc'ns, Inc., 393 F.3d 771 (8th Cir. 2005); *Verizon Internet Servs., Inc.*, 351 F.3d 1229.

69 17 U.S.C. § 512(h) (2006); *see also In re* Subpoena to Univ. of N.C. at Chapel Hill, 367 F. Supp. 2d 945, 958 (M.D.N.C. 2005) (referring to a DMCA subpoena as a "prelitigation subpoena").

70 17 U.S.C. § 512(h)(1)–(2).

71 *Id.* § 512(c)(3)(A)(iii).

Unlike § 512(i), which contains no reference on its face to § 512(c), but which has been interpreted nevertheless to incorporate that section's notice and "red flag" elements, § 512(h) *does* expressly incorporate § 512(c)'s notice element.[72] Whereas courts interpreting § 512(i) have construed it in a way that makes elements of § 512(c) applicable "through the back door" to § 512(a) providers, the D.C. Circuit and the Eighth Circuit have declined to read § 512(h) to do this.[73] In reaching the conclusion that the subpoena power in § 512(h) does not extend to § 512(a) providers, both courts found it dispositive that § 512(c)'s notice and takedown requirements apply on the face of the statute to providers that store information but not to those that act simply as a conduit for it.[74] This differentiation by function—host providers vs. conduit providers—makes sense considering that providers storing information for users have control over that information by virtue of the fact that it resides on their systems in a more-than-transient way.[75] Host providers are therefore able, as § 512(c)(3)(A) contemplates, to remove or disable access to that information upon notification that the information is infringing.[76] Providers that merely transmit information for users, by contrast, do not control the information that is being transmitted over their systems and cannot remove or disable access to it.[77] They can

[72] *See id.* § 512(h)(2)(A).

[73] *See Verizon Internet Servs., Inc.*, 351 F.3d at 1236 (holding that section 512(h) does not by its terms authorize the issuance of subpoenas to section 512(a) providers); *Charter Commc'ns, Inc.*, 393 F.3d at 777.

[74] *See Charter Commc'ns, Inc.*, 393 F.3d at 777 (holding that "because . . . Charter's function was limited to acting as a conduit for the allegedly copyright protected material, we agree § 512(h) does not authorize the subpoenas issued here"); *Verizon Internet Servs., Inc.*, 351 F.3d at 1236–37 ("We agree that the presence in § 512(h) of three separate references to § 512(c) and the absence of any reference to § 512(a) suggests the subpoena power of § 512(h) applies only to ISPs engaged in storing copyrighted material and not to those engaged solely in transmitting it on behalf of others.").

[75] *See Charter Commc'ns, Inc.*, 393 F.3d at 776 (explaining that each safe harbor that covers a function allowing the ISP to remove or disable access to infringing material (i.e., storage, system caching, or linking) contains a remove-or-disable access provision).

[76] *See id.* (explaining that each safe harbor provision that covers a function allowing the ISP to remove or disable access to content refers to the notification provision in section 512(c)); *In re* Subpoena to Univ. of N.C. at Chapel Hill, 367 F. Supp. 2d 945, 949 (M.D.N.C. 2005) (explaining that "[t]he notification in subsection (c)(3) presumes that the information is stored on a provider's system").

[77] *See Charter Commc'ns, Inc.*, 393 F.3d at 776 (explaining that the absence of the notification and remove-or-disable-access provisions from section 512(a) "makes sense where an ISP merely acts as a conduit for infringing material . . . because the ISP has no ability to remove the infringing material from its system or disable access to the infringing material").

terminate Internet access for specific users by blocking their IP addresses, as § 512(i) requires them to do, but they cannot disable access to the allegedly infringing material itself, as § 512(c) requires. Taking into account the necessary relationship between an ISP's control over stored information and its ability to remove or disable access to that information upon receipt of a DMCA-compliant notice, the D.C. Circuit held in *Recording Industry Ass'n of America, Inc. v. Verizon Internet Services, Inc.*[78] that "the text of § 512(h) and the overall structure of § 512 clearly establish . . . that § 512(h) does not authorize the issuance of a subpoena to an ISP acting as a mere conduit for the transmission of information sent by others."[79] The Eighth Circuit later reached the same conclusion in *In re Charter Communications, Inc.*[80]

With the conclusion that § 512(a) providers are not subject to the subpoena power created by § 512(h) because they do not store information for users, rights owners lost what would have been an efficient means of identifying infringing P2P file sharers for the purpose of initiating settlement negotiations or taking other steps to enforce their rights. Without the power to issue pre-litigation subpoenas to conduit ISPs under the authority of § 512(h), rights owners have been required to go to the trouble and expense of filing John Doe lawsuits in order to learn the identities of alleged infringers.[81] In the *Verizon* case, the RIAA argued that a narrow interpretation of § 512(h) "would defeat the core objectives" of the DMCA.[82] The court wrote that it was not unsympathetic to the need for legal tools to protect copyright owners from widespread infringement, but it could not, it said, rewrite the DMCA to provide

[78] *Verizon Internet Servs., Inc.*, 351 F.3d 1229.

[79] *Id.* at 1237.

[80] *Charter Commc'ns, Inc.*, 393 F.3d 771.

[81] After filing a "John Doe" lawsuit for copyright infringement, the copyright owner can subpoena the identity of the alleged infringer pursuant to Rule 45 of the Federal Rules of Civil Procedure. *See, e.g.*, Virgin Records Am., Inc. v. Doe, No. 5:08-CV-389-D, 2009 WL 700207 (E.D.N.C. Mar. 16, 2009) (denying the defendant's motion to quash a Rule 45 subpoena issued after the filing of a John Doe lawsuit alleging copyright infringement by means of a P2P network).

[82] *Verizon Internet Servs., Inc.*, 351 F.3d at 1238; *see also In re* Subpoena to Univ. of N.C. at Chapel Hill, 367 F. Supp. 2d 945, 953 (M.D.N.C. 2005) ("While the RIAA's argument at first blush is tempting, the Court rejects it because it would necessarily amount to the rewriting of the statute.").

for a technology that Congress had no reason to foresee when it drafted the statute.[83]

In a dissent from the Eighth Circuit's decision in the *Charter* case, Judge Murphy criticized the majority's decision "to block copyright holders from obtaining effective protection against infringement through conduit service providers."[84] He asserted that the majority's interpretation of § 512(h) "shields conduit ISPs from liability without requiring their assistance in protecting copyrights."[85] This contention is not strictly accurate, given that conduit ISPs in the wake of the *Verizon* and *Charter* decisions are still required to comply with subpoenas to identify alleged infringers when those subpoenas are issued in the context of pending litigation. There is no question, however, that the narrow interpretation of § 512(h) has made it both more time-consuming and more expensive for rights owners to enforce their copyrights in cases where the ISP acts only as a conduit and not as a host for the infringing material.[86]

E. The DMCA and the Prehistory of Graduated Response

Taken together, court decisions interpreting the DMCA and defining the specific obligations of ISPs seeking safe harbor under it have laid the groundwork for graduated response in two important ways. First, the decisions that interpret § 512(i) to incorporate § 512(c)'s notice and red flag provisions suggest that implementing a "three strikes and you're out" protocol or some near variant is sufficient, if not necessary, to qualify a conduit provider for safe harbor under § 512(a). While the decisions are silent as to how many "strikes" a given user should get before he or she is labeled a repeat infringer, and while they are equivocal as to what information must be counted by an ISP as a strike, they clearly establish that § 512(i) requires not only the adoption of a repeat infringer policy but also proof in the form of terminated or suspended users that the policy is actually enforced.

Second, the decisions interpreting § 512(h) to exclude conduit providers from the reach of pre-litigation subpoenas have foreclosed

---

[83] *Verizon Internet Servs., Inc.*, 351 F.3d at 1238.

[84] *Charter Commc'ns, Inc.*, 393 F.3d at 778 (Murphy, J., dissenting).

[85] *Id.* at 782.

[86] *See id.* (asserting that "John Doe actions are costly and time consuming" and that Congress did not intend that "copyright holders should be relegated to such cumbersome and expensive measures against conduit ISPs").

the statutory means by which rights owners could have made direct contact with alleged P2P infringers outside the context of litigation. This limitation has led rights owners to pursue private arrangements for "reaching through" to alleged P2P infringers. In 2005, the same year the Eighth Circuit decided *Charter*, Verizon entered into an agreement with Disney to forward notices of infringement, in return for which it received the right to transmit certain Disney programming over its network.[87] In late 2009, Verizon reached a notice-forwarding agreement with the RIAA.[88] In addition to these two agreements, Verizon is reportedly a party to a number of other, undisclosed agreements to forward notices on behalf of content providers.[89] Private arrangements such as these have the benefit for rights owners of being less public and more efficient than the filing of John Doe lawsuits. To the extent that copyright owners can convince conduit ISPs to serve as *their* conduits, forwarding notices of infringement to users whose IP addresses they have linked to infringing activity, they can communicate with alleged P2P infringers in a way that avoids litigation and obviates the privacy concerns associated with asking ISPs to disclose their users' identities.

Given users' resistance to the idea that their ISPs will embrace graduated response and begin functioning actively as Big Content's copyright cops, ISPs tend to tread very gingerly when it comes to public statements about their participation in graduated response programs. Representatives of major broadband providers including Comcast, Cox, and AT&T have denied publicly that they are participating in a "three strikes" program in cooperation with the RIAA.[90] At the same time, however, a Comcast executive disclosed that the company issues between one million and two million infringement notices per year to subscribers on behalf of copyright owners.[91] The executive, who couched his comments expressly in terms of DMCA compliance, said that forwarding notices of infringement to customers is nothing new for Comcast.[92] He also

[87] Nate Anderson, *Verizon to Forward RIAA Warning Letters (But That's All)*, ARS TECHNICA, Nov. 13, 2009, http://arstechnica.com/tech-policy/news/2009/11/verizon-to-forward-riaa-warning-letters-but-thats-all.ars.

[88] *Id.*

[89] *Id.*

[90] Albanesius, *supra* note 17.

[91] *Id.*

[92] *Id.*

acknowledged that Comcast has suspended the accounts of a small fraction of users in connection with the company's DMCA compliance efforts.[93] Cox representatives have admitted to having done the same in a small number of cases where repeated notices have gone unheeded by subscribers.[94] Verizon, for its part, has been equivocal concerning whether it has ever imposed service interruptions on alleged infringers.[95]

Although the impulse of broadband executives is to run the other way when they are confronted with questions from the media about "three strikes" and graduated response,[96] the fact of the matter is that broadband providers, in the name of the DMCA, have been engaged for a number of years in a form of graduated response *avant la lettre*: they have entered into arrangements with rights owners pursuant to which they forward notices of infringement to subscribers, and at least two major ISPs—Comcast and Cox—are on the record as having suspended access for subscribers who routinely receive and ignore such notices. Given the lack of clarity in court rulings interpreting § 512(i) as applied to conduit providers, what Comcast and Cox have done in cases where subscribers have ignored repeated notices is a cautious but not unreasonable approach to DMCA compliance.

Even when the lingering ambiguities concerning the precise obligations of conduit providers under § 512(i) are taken into account, it is plain on the face of the DMCA that no broadband provider can qualify for safe harbor if its policies do not provide for termination of access for repeat copyright infringers. This has been true since 1998. Accordingly, the terms of use for every major broadband provider contain a provision reserving the right to terminate access for any user

93 *Id.*

94 Sarah McBride, *Relationship Status of RIAA and ISPs: It's Complicated*, WALL ST. J., Mar. 26, 2009, http://blogs.wsj.com/digits/2009/03/26/relationship-status-of-riaa-and-isps-its-complicated/.

95 *See* Nate Anderson, *Verizon: We're Not Cutting Off Users Over Copyright Claims*, ARS TECHNICA, Jan. 21, 2010, http://arstechnica.com/tech-policy/news/2010/01/verizon-uh-we-arent-cutting-off-users-over-copyright-claims.ars (reporting that Verizon first admitted to and then denied having "cut some people off").

96 *See* David Kravets, *Top Internet Providers Cool to RIAA 3-Strikes Plan*, WIRED, Jan. 5, 2009, http://www.wired.com/threatlevel/2009/01/draft-verizon-o/ ("Two weeks after the Recording Industry Association of America announced it had struck deals with top internet service providers to cut off unrepentant music sharers, not a single major ISP will cop to agreeing to the ambitious scheme, and one top broadband company says it's not on board.").

who infringes copyrights.[97] Verizon and Comcast expressly reserve the right to do so unilaterally (i.e., in their "sole discretion"). In this sense, the most controversial element of graduated response, ISP-initiated termination of user access, has been part of the mix in online copyright enforcement for a good while, and the current controversy over the prospect that an ISP might suspend a user's access for repeated violations of copyright law seems belated.

II

"MERE CONDUITS" NO MORE: BROADBAND PROVIDERS, INTELLIGENT NETWORKS, AND THE END OF PASSIVE CARRIAGE

What *is* relatively new, however, and what is changing the post-DMCA copyright enforcement calculus for content owners, broadband providers, and their customers is the increasingly routine deployment of "smart" technology within broadband networks.[98]

[97] *See, e.g.*, *AT&T High Speed Internet Terms of Service*, AT&T, http://www.att.net/csbellsouth/s/s.dll?spage=cg/legal/att.htm&leg=tos (last updated June 14, 2009) ("AT&T may, however, immediately terminate or suspend your Member Account and Sub Accounts, and all or a portion of your Service without notice if . . . you . . . engage in conduct that is a violation of any law, regulation or tariff (including, without limitation, copyright and intellectual property laws)."); *Comcast Acceptable Use Policy For High-Speed Internet Services*, COMCAST.NET, http://www.comcast.net/terms/use/ (last updated Jan. 1, 2009) [hereinafter *Comcast Acceptable Use Policy*] ("It is Comcast's policy in accordance with the DMCA and other applicable laws to reserve the right to terminate the Service provided to any customer or user who is either found to infringe third party copyright or other intellectual property rights, including repeat infringers, or who Comcast, in its sole discretion, believes is infringing these rights. Comcast may terminate the Service at any time with or without notice for any affected customer or user."); *Verizon Internet Access Terms of Service*, VERIZON, http://www.verizon.net/central/vzc.portal?_nfpb=true&_pageLabel=vzc_help_policies&id=TOS (last updated Jan. 17, 2010) [hereinafter *Verizon Terms of Service*] ("In accordance with the Digital Millennium Copyright Act (DMCA) and other applicable laws, it is the policy of Verizon to suspend or terminate, in appropriate circumstances, the Service provided to any subscriber or account holder who is deemed to infringe third party intellectual property rights, including repeat infringers of copyrights. In addition, Verizon expressly reserves the right to suspend, terminate or take other interim action regarding the Service of any Subscriber or account holder if Verizon, in its sole judgment, believes that circumstances relating to an infringement of third party intellectual property rights warrant such action.").

[98] As Paul Ohm explains:

> Because ISPs have the means, thanks to recent advances in monitoring technology, motive—financial turmoil coupled with pressures to use new technologies to raise revenue and assist third parties—and opportunity—ownership of the network bottleneck—they have begun to embrace new forms of aggressive monitoring. In the past year in particular, the headlines have been

Technologies like deep packet inspection (DPI) have given broadband operators an unprecedented level of control over the content that flows through their "pipes."[99] DPI gives broadband providers the ability to look beyond the header of a data packet, which contains routing information, and into the packet's payload, which is the actual data inside the packet.[100] The uses of DPI are multifarious, and the reasons for which broadband providers have implemented the technology are at most tangentially related to copyright enforcement. DPI can be used, for example, for detection and filtering of viruses and malware, management of network congestion (which is caused, in part, by P2P traffic), traffic sorting (in support of service tiering or prioritization), and data mining (in support of behavioral advertising).[101] It can also be used for law enforcement purposes, as required by the Communications Assistance to Law Enforcement Act (CALEA), to capture and transmit data to government agents.[102]

Although copyright enforcement is not the reason for which broadband operators have implemented DPI technology within their networks, blocking unauthorized transmissions of copyrighted content

> filled with stories about ISPs conducting or proposing invasive new monitoring. This has happened at a breathtaking pace and suggests an undeniable trend.

Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417, 1432 (2009).

The powerful surveillance tools to which Ohm refers are the product of a technological evolution in network intelligence that began in the early 2000s. *See, e.g.*, Mark A. Lemley & Lawrence Lessig, *The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era*, 48 UCLA L. REV. 925, 939 (2001) ("While the [end-to-end] architecture of the Internet is fundamentally in place, users and network administrators are introducing intelligence into the network for a variety of reasons. Firewalls, proxy servers, Network Address Translators (NATs), and other systems are designed to determine the content and origin of packets and discriminate between packets.").

99 *See* Matt Villano, *Peering Deeply into Network Traffic*, CRN, June 28, 2004, http://www.crn.com/security/22101663;jsessionid=BC10PXZ1W2T2DQE1GHPSKHWATMY32JVN ("This new technology, dubbed deep-packet inspection, scans every bit and byte of every piece of data as it crosses the network perimeter.").

100 Nate Anderson, *Deep Packet Inspection Meets 'Net Neutrality, CALEA*, ARS TECHNICA, July 25, 2007, http://arstechnica.com/hardware/news/2007/07/Deep-packet-inspection-meets-net-neutrality.ars.

101 *See id.*

102 *See Communications Assistance for Law Enforcement Act (CALEA)*, FED. COMM. COMMISSION, http://www.fcc.gov/calea/ (last updated Feb. 21, 2007) ("CALEA was intended to preserve the ability of law enforcement agencies to conduct electronic surveillance by requiring that telecommunications carriers and manufacturers of telecommunications equipment modify and design their equipment, facilities, and services to ensure that they have the necessary surveillance capabilities.").

is a potential application for DPI.[103] Using DPI, ISPs have the ability to automate and centralize the previously dispersed processes of monitoring, notice, and termination, which are the essential elements of graduated response.[104] Paul Ohm predicts that ISPs, in response to technological changes and a desire to increase revenue, will use DPI to monitor more aggressively as time goes on, absent some regulatory or non-regulatory intervention.[105] It is likely that copyright enforcement, for the reasons discussed below, will become part of this expanded monitoring trend.

A key element of the negotiation strategy for rights owners seeking to partner with broadband providers in the implementation of a network-level solution to online piracy is the assertion that management of P2P traffic should be regarded as a matter of shared concern. Content owners, not without success, have been selling the idea that broadband operators can help themselves manage network congestion by helping rights owners combat infringement.[106] Comcast's highly controversial use of DPI in 2007 to throttle BitTorrent traffic is one manifestation of the coincidental community of interest that has developed between rights owners and network

103 *See What Your Broadband Provider Knows About Your Web Use: Deep Packet Inspection and Communications Laws and Policies: Hearing Before the Subcomm. on Telecomms. and the Internet of the H. Comm. on Energy and Commerce*, 110th Cong. 7 (2008) (statement of Alissa Cooper, Chief Computer Scientist, Center for Democracy & Technology), *available at* http://energycommerce.house.gov/images/stories/Documents/Hearings/PDF/Testimony/TI/110-ti-hrg.071708.Cooper-testimony.pdf (listing detection of intellectual property among the many applications for DPI).

104 Audible Magic markets a deep packet inspection appliance to colleges and universities that is tailored specifically to on-campus copyright enforcement. *See The Graduated Response System*, AUDIBLE MAGIC, http://www.audiblemagic.com/products-services/copysense/graduated-response.asp (last visited Oct. 2, 2010) ("The Graduated Response system fully supports the three-strikes policies in place at many colleges and universities. The [system] . . . automatically communicates graduating levels of responses. . . . The more times a user is caught, the more severe the sanctions. Sanctions can also include the automatic blocking of network access for a particular user for a specified and graduated period of time.").

105 Ohm, *supra* note 98, at 1436–37.

106 *See* Saul Hansell, *Hollywood Wants Internet Providers to Block Copyrighted Files*, N.Y. TIMES, Sept. 25, 2008, http://bits.blogs.nytimes.com/2008/09/25/hollywood-tries-to-get-support-for-having-isps-block-copyrighted-files/ (explaining that Internet providers like AT&T are potentially interested in content filtering as a way to reduce network traffic caused by the trading of video files); Brad Stone, *AT&T and Other I.S.P.'s May Be Getting Ready to Filter*, N.Y. TIMES, Jan. 8, 2008, http://bits.blogs.nytimes.com/2008/01/08/att-and-other-isps-may-be-getting-ready-to-filter/ (reporting on talks at the Consumer Electronics Show between representatives of NBC, Microsoft, AT&T, and content filtering companies).

operators with respect to the use of smart network technology to manage bandwidth-intensive P2P traffic. In late 2007, Comcast was discovered to have been blocking BitTorrent transfers as a means of congestion management.[107] In 2008, Comcast was sanctioned for this conduct by the FCC, though it argued in the proceedings that it was simply engaged in "legitimate network management."[108]

While the use of DPI for copyright enforcement purposes goes a giant step beyond ISPs' existing agreements to forward notices of infringement on behalf of rights owners, there is a compelling legal reason for ISPs to consider the prospect seriously. As broadband providers have abandoned the end-to-end model of data transit[109] in favor of intrusive traffic management or shaping, their continuing eligibility for the "mere conduit" safe harbor in § 512(a) has become questionable.[110] To the extent that their network management practices now entail active intervention at the level of content,[111] ISPs have exposed themselves to copyright liability from which § 512(a) shielded them when they were content to be "dumb pipes."[112] The

107 Bridy, *supra* note 8, at 598–99.

108 *See id.* at 599.

109 *See, e.g.*, Jon M. Peha, *The Benefits and Risks of Mandating Network Neutrality, and the Quest for a Balanced Policy*, 1 INT'L J. OF COMM. 644, 646 (2007), *available at* http://ijoc.org/ojs/index.php/ijoc/article/viewFile/154/90 ("Traditionally, Internet packets were sent with equal priority and 'best effort,' i.e., with no guarantee of delivery. . . . Times have changed. There are a variety of techniques through which networks can now favor some packets or packet streams over others.")

110 *See* Frieden, *supra* note 18, at 645.

111 According to Sandvine, a Canadian provider of DPI hardware to ISPs worldwide, ninety percent of its 160 ISP customers use the technology to manage traffic on their networks. Nate Anderson, *DPI Vendor Says 90% of ISP Customers Engage in Traffic Discrimination*, ARS TECHNICA, Aug. 3, 2009, http://arstechnica.com/tech-policy/news/2009/08/network-neutrality-dead-in-practice-as-most-isps-throttle.ars.

The terms of service for Cox Communications high-speed Internet subscribers contain a network management provision that implies the use of DPI:

> Network management may include, without limitation, the following actions: rate limiting of email (as set forth in our email policies), rejection or removal of "spam" or otherwise unsolicited bulk email, port blocking, cybersecurity mechanisms (including identification and blocking of viruses, phishing sites and other malware), measuring subscriber bandwidth usage, traffic prioritization and protocol filtering.

Cox Communications Policies: Subscriber Agreement, COX COMMUNICATIONS, http://ww2.cox.com/aboutus/policies.cox#sub (last updated July 1, 2010) [hereinafter *Cox Communications Subscriber Agreement*].

112 *See* 17 U.S.C. § 512(a)(2), (b)(2)(A) (2006) (conditioning safe harbor eligibility on an ISP's routing of data "without selection of the material by the service provider" and "without modification to its content").

subsections that follow provide a brief history of common carriage, a discussion of copyright law's special rules of (non)liability for passive carriers, and an exploration of the liability effects of ISPs' transition to a "smart" model of data transit.

A. Common Carriage Historically

The IITF's analogy between conduit ISPs and the telephone company was particularly appropriate in the days before cable and fiber broadband, when users connected to the Internet via narrowband dial-up connections that used existing telephone lines to transmit data.[113] Although the Internet in those days represented a technological advance so revolutionary that it seemed to some to defy regulation,[114] it relied absolutely at its inception on an existing physical infrastructure whose operators (i.e., telephone companies) were subject to a quite old-fashioned regulatory paradigm: common carriage.[115] Given the early Internet's dependence on the telephone network, it is no surprise that the IITF and policy makers were eying the novel problem of copyright liability for ISPs through the familiar lens of common carriage. A brief discussion of the history of common carrier regulation therefore provides a useful context for understanding the origins of the DMCA's safe harbor for service providers that transmit or route materials for their customers (i.e., conduit ISPs).

---

[113] *See* FED. TRADE COMM'N, BROADBAND CONNECTIVITY COMPETITION POLICY: FTC STAFF REPORT JUNE 2007, at 19 (2007), *available at* http://www.ftc.gov/reports/broadband/v070000report.pdf [hereinafter FTC STAFF REPORT] (explaining that "[f]rom [the Internet's] creation to its early commercialization, most computer users connected . . . using a 'narrowband' dial-up telephone connection and a special modem to transmit data over the telephone system's traditional copper wirelines"); *see also* Religious Tech. Ctr. v. Netcom On-line Commc'n Servs., Inc., 907 F. Supp. 1361, 1365 n.2 (N.D. Cal. 1995) (describing the Internet as "a collection of thousands of local, regional, and global Internet Protocol networks . . . tied together via telephone lines" (quoting David Bruning, *Along the InfoBahn*, ASTRONOMY, June 1995, at 74, 76)).

[114] *See, e.g.*, David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1370 (1996) (asserting that the Internet "radically subverts the system of rule-making based on borders between physical spaces").

[115] Kevin Werbach has characterized common carriage as "[t]he dominant communications regulatory paradigm of the twentieth century." Kevin Werbach, *Only Connect*, 22 BERKELEY TECH. L.J. 1233, 1246 (2007).

The Communications Act of 1934, which created the FCC to regulate the nation's growing telephone and telegraph industries,[116] defined "common carrier" circularly: "The term 'common carrier' . . . means any person engaged as a common carrier for hire, in interstate or foreign communication by wire or radio."[117] The unhelpful circularity of the statutory definition has been noted by academics and judges alike.[118] Phil Nichols has attributed it to the existence of an ordinary meaning of "common carrier" in 1934, such that Congress saw no need to define it expressly in the statute.[119] Whatever the Congressional motivation for failing to provide a precise definition of the term, courts were predictably called upon to fill the void, and they did so through recourse to the common law of common carriage.[120]

At early common law, an assortment of businesses, including innkeepers, railroads, warehouses, package carriers, and ferry operators, were classified as common carriers.[121] For the most part, these businesses, as the term denotes, carried people or goods from one place to another.[122] Those not engaged in the act of carriage itself, for example innkeepers and warehouses, had a direct connection to the means of transportation or communication and, thereby, a close practical relationship to actual carriers.[123] Historically, the essential attributes of common carriage have been nondiscriminatory access for all served and indifference to the nature

116 Susan Crawford discusses the passage of the Communications Act of 1934 in terms of the perceived failure of the Interstate Commerce Commission, whose job was mainly regulating the railroads, to attend to communications regulation, which had become its responsibility under the Mann-Elkins Act of 1910. *See* Susan P. Crawford, *Transporting Communications*, 89 B.U. L. REV. 871, 880–81 (2009).

117 47 U.S.C. § 153(10) (2006).

118 *See, e.g.*, Fed. Commc'ns Comm'n v. Midwest Video Corp., 440 U.S. 689, 701 n.10 (1979); Fed. Trade Comm'n v. Verity Int'l, Ltd., 443 F.3d 48, 57 (2d Cir. 2006); Werbach, *supra* note 115, at 1247.

119 Phil Nichols, *Redefining 'Common Carrier': The FCC's Attempt at Deregulation by Redefinition*, 1987 DUKE L.J. 501, 511 (1987) ("The facial circularity of contemporary definitions of common carrier suggests that there was indeed an 'ordinary sense' of the phrase, so that Congress did not believe it needed to provide a precise definition.").

120 Nat'l Ass'n of Regulatory Util. Comm'rs v. Fed. Commc'ns Comm'n, 533 F.2d 601, 608 (D.C. Cir. 1976) (stating that "the circularity and uncertainty of the common carrier definitions set forth in the statute and regulations invite recourse to the common law of carriers").

121 Werbach, *supra* note 115, at 1246.

122 Thomas B. Nachbar, *The Public Network*, 17 COMMLAW CONSPECTUS 67, 76 (2008), *available at* http://commlaw.cua.edu/res/docs/06_Nachbar.pdf.

123 *See id.* at 102.

of the goods carried.[124] These two requirements—frequently conflated under the rubric of nondiscrimination—have remained constant over time, even as the means of carriage have evolved and the nature of goods carried has become less tangible. Whether the subject of carriage is tangible goods or electrical pulses, both at common law and in the regulatory framework that developed in its wake, control over the destination and contents of a "package" in the hands of a common carrier is, and at all times remains, with the sender. In other words, the definitive function of the common carrier is passive transportation of someone else's stuff.

B. Common Carriage and Broadband Access Providers

Controversially, ISPs—including cable, DSL, and wireless broadband providers—have not been subject to the common carrier requirements that define the regulatory space for wire-based telephony.[125] This (de)regulatory choice lies at the heart of the long-

[124] *See* Fed. Trade Comm'n v. Verity Int'l, Ltd., 443 F.3d 48, 58 (2d Cir. 2006) (explaining that "the definition of a common carrier coalesced into two requirements: (1) the entity holds itself out as undertaking to carry for all people indifferently; and (2) the entity carries its cargo without modification"); *see also* Nachbar, *supra* note 122, at 107 ("Nondiscrimination has been implemented almost exclusively with regard to delivery of undifferentiated services, such as carriage . . . . The identity of the transported good is largely irrelevant."); Werbach, *supra* note 115, at 1246 (explaining that "[a] common carrier cannot . . . differentiate in the treatment of similarly situated customers, evaluate the content of what it receives from its customers, or refuse to serve interested customers, even when that means building out its facilities to reach them").

[125] *See* Crawford, *supra* note 116, at 901–02. This state of affairs may change in the near future. In June 2010, the FCC issued a notice of inquiry (NOI) seeking comment on the possible reclassification of the connectivity component of broadband service as a telecommunications service under Title II of the Telecommunications Act. *See Notice of Inquiry: In the Matter of Framework for Broadband Internet Service Before the Fed. Commc'ns Comm'n*, GN Docket No. 10-127 (2010), *available at* http://www.fcc.gov/Daily_Releases/Daily_Business/2010/db0617/FCC-10-114A1.pdf [hereinafter *Notice of Inquiry*].

The NOI seeks to define a "third way" between the aggressive regulation that has applied historically to wire line phone carriers and the essentially non-regulatory approach to broadband taken by the FCC during the Bush era. *See id.* at 2 (seeking public comment on "a third way under which the Commission would . . . reaffirm that Internet *information* services should remain generally unregulated [and] identify the Internet *connectivity* service that is offered as part of wired broadband Internet service (and only this connectivity service) as a telecommunications service" (emphasis added)). The meaning and potential consequences of the proposed reclassification are discussed below, in this subsection.

running net neutrality debate.[126] Susan Crawford has intricately traced the demise of common carriage in the telecommunications context, a development that she finds troubling given the concept's foundational place in telecommunications policy for the last 150 years.[127] This subsection contains an abbreviated version of the story Crawford tells, followed by an account of some important recent developments on the regulatory front.

In 1996, when the Communications Act of 1934 was overhauled to bring it up to date with developing technologies, telephone companies were regulated as common carriers.[128] When narrowband Internet access evolved into broadband access and phone companies began offering high-speed DSL service over their existing wire lines, they were still treated as common carriers.[129] Cable operators, by contrast, were never regulated as common carriers.[130] They were subject to a "light-touch" regulatory regime, because they were viewed as entertainment broadcasters that were not using public airwaves and were thus not subject to the public trustee obligations of over-the-air broadcasters.[131] In addition, they functioned as one-way pipes, so they escaped common carriage requirements to which telephone companies were subjected as operators of two-way communications networks.[132]

When cable operators began providing broadband Internet access, the FCC did not treat them for regulatory purposes in the same way that it treated DSL operators, which had inherited legacy common carriage obligations as a function of their historical provision of telephone services. Instead, the FCC continued to treat cable companies as it had before their entry into the two-way communications business.[133] In its landmark decision in *National*

126 The contours of this debate are beyond the scope of this Article and have been well delineated elsewhere. *See, e.g.*, FTC STAFF REPORT, *supra* note 113; Tim Wu, *The Broadband Debate, A User's Guide*, 3 J. ON TELECOMM. & HIGH TECH. L. 69 (2004).

127 Crawford, *supra* note 116, at 876 (arguing that "[c]urrent general-purpose communications law is failing us" because it "does not include non-discriminatory access to general-purpose communications").

128 *Id.* at 901.

129 *Id.*

130 *Id.* at 901–02.

131 *Id.* at 902.

132 *Id.*

133 *See, e.g.*, Adam Thierer, *Are "Dumb Pipe" Mandates Smart Public Policy? Vertical Integration, Net Neutrality, and the Network Layers Model*, 3 J. ON TELECOMM. & HIGH TECH. L. 275, 280 (2005) (explaining that "telephone companies are governed under Title

Cable & Telecommunications Ass'n v. Brand X Internet Services,[134] the Supreme Court upheld the FCC's declaratory ruling that cable operators of broadband networks should be classified for regulatory purposes as information services and not as telecommunications services.[135] The latter are subject to regulation under Title II of the Telecommunications Act of 1996; the former are not. The import of this decision was to exempt cable operators of broadband services from common carrier obligations, which are built into the statutory definition of telecommunications: "The term 'telecommunications' means the transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received."[136] Classification of cable broadband as an information service freed cable companies to manage the content flowing across their networks in ways that are not permitted to common carriers. It also raised the stakes in the debate over net neutrality, with advocates of a free and open Internet predicting a new era of corporate control over online content.

The *Brand X* decision, which reversed the Ninth Circuit's holding that cable broadband service should be classified as a "telecommunications service" subject to mandatory Title II common carrier regulation,[137] implicitly ratified an asymmetry in the regulation of broadband providers. Following *Brand X*, cable broadband providers and DSL broadband providers were classified differently for regulatory purposes, despite the similarity in the services they provided (i.e., high-speed Internet access). DSL broadband providers remained subject to legacy regulation as common carriers; cable broadband providers, classified as "information services," were exempt from Title II requirements. Parity between the two types of providers was achieved, however, when the FCC ruled in 2005 that DSL broadband is also an "information service" within the meaning of the Telecommunications

II of the Communications Act as common carriers . . . while cable providers operate under Title VI" and are not subject to common carrier obligations).

134 Nat'l Cable & Telecomms. Ass'n v. Brand X Internet Servs., 545 U.S. 967 (2005).

135 *Id.* at 997 (holding that the FCC's decision was a reasonable policy choice in light of a textual ambiguity in the Telecommunications Act).

136 47 U.S.C. § 153(43) (2006).

137 Brand X Internet Servs. v. Fed. Commc'ns Comm'n, 345 F.3d 1120, 1129 (9th Cir. 2003) (holding that "the transmission element of cable broadband service constitutes telecommunications service under the terms of the Communications Act").

Act.[138] That ruling was followed in 2007 by a ruling that broadband Internet access over wireless networks is also an "information service" for regulatory purposes.[139] Taken together, *Brand X* and the two subsequent administrative rulings covering DSL and wireless effectively mark the end of telecommunications common carriage in the context of broadband Internet access.

These rulings mean that all broadband providers, uniformly classified as "information services," are relieved of the nondiscrimination requirements statutorily imposed on "telecommunications services" as common carriers under Title II.[140] Citing the FCC's continuing authority to regulate broadband under Title I of the Telecommunications Act, FCC Chairman Julius Genachowski issued the Open Internet NPRM, mentioned in passing in the opening paragraph of this Article, in October 2009. When the rule-making began, Comcast's appeal of the FCC sanction imposed on it for blocking BitTorrent traffic was pending in the Court of Appeals for the D.C. Circuit.[141] In the appeal, Comcast challenged the FCC's Title I jurisdiction to regulate cable broadband, despite dicta from *Brand X* stating that the FCC retained ancillary jurisdiction under Title I to "impose special regulatory duties on facilities-based ISPs."[142]

In a decision that pulled the rug out from under the FCC and the Open Internet NPRM, the D.C. Circuit decided the appeal in favor of Comcast.[143] The panel held that the FCC, which premised its assertion of jurisdiction over Comcast on the Supreme Court's dicta in *Brand X*, "stretche[d] the Court's words too far . . . [b]y leaping from [the] observation that the Commission's ancillary authority may allow it to impose *some* kinds of obligations on cable Internet providers to a claim of plenary authority over such providers."[144] The D.C. Circuit's conclusion that the FCC lacks statutorily delegated

138 *See* Appropriate Framework for Broadband Access to the Internet over Wireline Facilities, 20 FCC Rcd. 14853 (2005).

139 *See* In the Matter of Appropriate Regulatory Treatment for Broadband Access to the Internet Over Wireless Networks, 22 FCC Rcd. 5901 (2007).

140 They are relieved of other obligations as well. *See Brand X Internet Servs.*, 545 U.S. at 975 (explaining that telecommunications carriers must charge just, reasonable, nondiscriminatory rates to customers, design their networks so that other carriers can interconnect with them, and contribute to the federal universal service fund).

141 *See* Comcast Corp. v. Fed. Commc'ns Comm'n, 600 F.3d 642 (2010).

142 *Brand X Internet Servs.*, 545 U.S. at 996.

143 *Comcast Corp.*, 600 F.3d at 661.

144 *Id.* at 650.

authority to regulate cable broadband providers under Title I has left the FCC to decide whether to reclassify broadband as a telecommunications service and thereby claim jurisdiction to regulate it under Title II.[145]

The prospect of reclassification is controversial both within the FCC and in Congress,[146] and broadband providers moved quickly after the *Comcast* decision to state publicly their view that any future action on broadband regulation should be a matter for Congress, not the FCC.[147] In the thick of the fallout from *Comcast*, the FCC issued a notice of inquiry (NOI) proposing to reclassify only the connectivity component of broadband service as a Title II telecommunications service, leaving the information component unregulated.[148] In the

145 Following the D.C. Circuit's decision, the FCC issued a statement conceding that the decision "invalidated the prior Commission's approach to preserving an open Internet." Press Release, Fed. Commc'ns Comm'n, FCC Statement on Comcast v. FCC Decision (Apr. 6, 2010), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-297355A1.pdf. The statement also asserted, however, that the court did not "close the door to other methods for achieving this important end." *Id.* In a separately issued statement, Commissioner Michael Copps was less elliptical about the FCC's options: "The only way the Commission can make lemonade out of this lemon of a decision is to do now what should have been done years ago: treat broadband as the telecommunications service that it is." Press Release, Fed. Commc'ns Comm'n, Statement of Commissioner Michael J. Copps on the Comcast v. FCC Decision (Apr. 6, 2010), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-297368A1.pdf.

146 *See* Press Release, Fed. Commc'ns Comm'n, Statement of Commissioner Robert M. McDowell on the Recent D.C. Circuit Court of Appeals Decision in the Comcast/BitTorrent Case (Apr. 6, 2010), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-297364A1.pdf ("I hope this decision . . . will not lead to the unnecessary classification of broadband service as a monopoly phone service under Title II of the Act."). Republican Senator Kay Bailey Hutchison of Texas, the Senate Commerce Committee's ranking minority member, also spoke out against reclassification, asserting that the FCC could not act without approval from Congress. Edward Wyatt, *Despite Ruling, F.C.C. Says It Will Move Forward on Expanding Broadband*, N.Y. TIMES, Apr. 14, 2010, http://www.nytimes.com/2010/04/15/technology/15broadband.html?hpw.

147 *See* Margaret Boles, *AT&T on Comcast v. FCC Decision*, AT&T PUB. POLICY BLOG (Apr. 6, 2010, 3:23 PM), http://attpublicpolicy.com/uncategorized/att-statement-on-comcast-v-fcc-decision/ (stating AT&T's position that the FCC should look to Congress for clarification concerning its jurisdiction over broadband providers).

148 *See Notice of Inquiry*, *supra* note 125, at 2 (outlining three alternative approaches to regulating broadband service). The connectivity component of broadband service consists of "establishing a physical connection to the Internet and interconnecting with the Internet backbone," as well as performing other functions that enable the transmission of data. *Id.* at 8. The information component consists of such services as e-mail, access to online newsgroups, and the ability to create a personal Web page. *See id.* In *Brand X*, the Supreme Court affirmed the FCC's decision to treat the two components as unitary for regulatory purposes, subsuming them both under the rubric of information services. The FCC now proposes to "unbundle" them for regulatory purposes.

NOI, the FCC attempts to map a "third way" between reclassifying broadband "as a 'telecommunications service' to which the full weight of Title II requirements would apply" and maintaining its current classification as a unitary information service to which no Title II requirements apply.[149] In keeping with the aim of finding a middle ground between heavy regulation and no regulation, the NOI tempers the potentially onerous consequences of reclassification with the promise that the FCC will "forbear . . . from applying all provisions of Title II other than the small number that are needed to implement the fundamental universal service, competition and small business opportunity, and consumer protection policies that have received broad support."[150] The "third way" thus represents a species of light touch Title II regulation—a novel regulatory hybrid that offers an elegant solution to the perennial (and perennially vexing) problem of how to adapt old law to new technology.

It is too soon to tell what the outcome of the NOI will be, or, indeed, whether the administrative process it began will be interrupted or preempted by legislative intervention. If reclassification along the lines of the "third way" does occur, the FCC is unlikely to promulgate rules that altogether prohibit broadband providers from actively managing traffic on their networks. The more probable scenario is that the FCC would exercise newly claimed Title II jurisdiction to move forward with the draft rules already proposed in the Open Internet NPRM,[151] two of which specifically govern how broadband providers carry content for their customers:

> §8.5 Content.
>
> Subject to reasonable network management, a provider of broadband Internet access service may not prevent any of its users from sending or receiving the lawful content of the user's choice over the Internet.[152]
>
> §8.13 Nondiscrimination.
>
> Subject to reasonable network management, a provider of broadband Internet access service must treat lawful content, applications, and services in a nondiscriminatory manner.[153]

[149] *Id.* at 13.

[150] *Id.* at 2.

[151] *See* Preserving the Open Internet, Broadband Industry Practices, 74 Fed. Reg. 62638, 62661 (proposed Nov. 30, 2009) (to be codified at 47 C.F.R. pt. 8).

[152] *Id.* (to be codified at 47 C.F.R. pt. 8.5).

[153] *Id.* (to be codified at 47 C.F.R. pt. 8.13).

The mandates in all six of the proposed rules, including the two quoted above, are "subject to reasonable network management," which is defined to include "reasonable practices employed . . . [to] reduce or mitigate the effects of congestion . . . or to address quality-of-service concerns . . . [or to] [p]revent the unlawful transfer of content."[154] The across-the-board allowance in the draft rules for "reasonable network management" is a clear sign that the FCC does not contemplate a wholesale return to a regime of mandatory passive carriage.

Most relevant to the project of online copyright enforcement, broadband providers have leeway under the draft rules to prevent the unlawful transfer of content, an exception that seems designed to permit monitoring and blocking of infringing file transfers.[155] In their formal comments to the FCC in response to the notice of proposed rule-making, trade groups representing corporate rights owners predictably expressed enthusiastic support for the network management exception as it relates to unlawful file transfers.[156] In remarks to the National Association of Broadcasters during the week following the D.C. Circuit's decision in *Comcast*, Chairman Genachowski took care to communicate to the audience his belief that net neutrality and online copyright enforcement are not mutually exclusive ends; in the space of a single sentence, he invoked both the importance of a free and open Internet and the need of broadcasters to prevent online copyright infringement.[157]

---

[154] *Id.* (to be codified at 47 C.F.R. pt. 8.3).

[155] *Id.* at 62650 ("In order for network openness obligations and appropriate enforcement of copyright laws to co-exist, it appears reasonable for a broadband Internet access service provider to refuse to transmit copyrighted material if the transfer of that material would violate applicable laws.").

[156] *See Comments of the Motion Picture Association of America, Inc. in the Matter of Preserving the Open Internet Broadband Industry Practices: Before the Fed. Commc'ns Comm'n*, GN Docket No. 09-191, at ii (2010) ("MPAA urges the Commission, as it considers its approach to network neutrality, to make clear that ISPs are not only permitted, but encouraged, to work with content owners to employ the best available tools and technologies to combat online content theft."); *Comments of the Recording Industry Association of America in the Matter of Preserving the Open Internet Broadband Industry Practices: Before the Fed. Commc'ns Comm'n*, GN Docket No. 09-191, at 13 (2010), *available at* http://fjallfoss.fcc.gov/ecfs/document/view?id=7020376700 ("We thus urge the Commission to adopt rules that not only allow ISPs to address online theft, but actively encourage their efforts to do so. Crucial to this project, the Commission must ensure that its Open Internet rules do not have a chilling effect on such efforts.").

[157] Julius Genachowski, Chairman, Fed. Commc'ns Comm'n, National Association of Broadcasters Show 2010, at 3 (Apr. 13, 2010), *available at* http://hraunfoss.fcc.gov/edocs

While the rules proposed in the Open Internet NPRM would not require ISPs to block any file transfers, and while the DMCA clearly establishes that qualifying ISPs have no affirmative duty to monitor their services for transfers of infringing content, engagement by broadband providers in active network management changes their relationship to the material they carry for their customers in ways that have implications for the special rules of liability they enjoyed when they acted as mere conduits.

C. Common Carriers and Copyright Liability

The affinities between the common law definition of a common carrier, the statutory definition of "telecommunications," and the DMCA's definition of a qualifying § 512(a) Internet service provider are apparent. The emphasis in all three definitions is on the passive role of the carrier and the sender's total dominion over both the destination and the contents of the transmission. While the DMCA never uses the term "common carrier," and while the narrowband access providers that existed when the statute was enacted were never regulated as common carriers by the FCC,[158] the language of § 512(a) and (k) is firmly rooted in the tradition of common carriage.

The policy underlying § 512(a)—that providers acting as passive conduits and automatically transmitting material chosen by others should not be held liable if that material turns out to be infringing—was not without antecedent in copyright law when the DMCA was enacted in 1998. Section 111 of the Copyright Act of 1976, which established a compulsory licensing scheme for cable systems that retransmit copyrighted programming, also accords special treatment to passive carriers.[159] Before § 111 was enacted, cable operators paid no copyright royalties, even though they retransmitted copyrighted

_public/attachmatch/DOC-297469A1.pdf ("I believe it's vital that the Internet remain free and open for content creators like you to innovate and reach your audience, and vital also that you can protect your content online against unlawful copyright infringement.").

158 As the Ninth Circuit has explained,

> [a] conventional dial-up ISP provides its subscribers access to the Internet at a "point of presence" assigned a unique Internet address, to which the subscribers connect through telephone lines. The telephone service linking the user and the ISP is classic "telecommunications" [subject to common carriage regulations]. . . . By contrast the FCC considers the ISP as providing "information services" under the Act.

Brand X Internet Servs. v. Fed. Commc'ns Comm'n, 345 F.3d 1120, 1128–29 (9th Cir. 2003) (quoting AT&T Corp. v. City of Portland, 216 F.3d 871, 877 (9th Cir. 2000)).

159 *See* 17 U.S.C. § 111(a)–(d) (2006).

over-the-air programming to the public.[160] Under the licensing scheme in § 111, cable systems pay a semiannual fee to the Register of Copyrights, in return for which they receive a license.[161] The fees collected from the cable systems are then distributed to copyright owners by the Copyright Royalty Board.[162]

In addition to exempting local and network programming from the scope of liability for unlicensed retransmission by cable systems, Congress in § 111 exempted intermediary carriers that act "as a communications conduit between the distant broadcast station and interested cable systems."[163] To qualify for the exemption, a carrier must establish that it has "no direct or indirect control over the content or selection of the primary transmission or over the particular recipients of the secondary transmission" and that its "activities with respect to the secondary transmission consist solely of providing wires, cables, or other communications channels for the use of others."[164] In the § 111 analysis, the carrier's nonintervention in the contents of the communication is a critical element: "To remain exempt, a carrier-retransmitter must avoid content control by retransmitting exactly what and all of what it receives . . . . To do otherwise could be perceived as the carrier's making the transmission its own."[165] Leaping forward twenty-two years to the DMCA, § 512(a) and (k) make the same requirement applicable to conduit ISPs seeking safe harbor: § 512(a) mandates that "the material is transmitted through the system or network without modification of its content."[166] Section 512(k) somewhat redundantly requires that a qualifying ISP provide routing and transmission "without modification to the content of the material as sent or received."[167]

Case law interpreting § 111 has held that the exemption is not limited to common carriers per se, but rather applies more broadly to

160 Hubbard Broad., Inc. v. S. Satellite Sys., Inc., 777 F.2d 393, 395 (8th Cir. 1985).

161 *Id.*

162 *Id.* The Copyright Royalty Tribunal, to which the *Hubbard* decision refers, was replaced in 1993 by the Copyright Arbitration Royalty Panel (CARP), which was itself replaced in 2004 by the Copyright Royalty Board (CRB). *See* U.S. Copyright Office, *Copyright Arbitration Royalty Panels (CARP)*, COPYRIGHT, http://www.copyright.gov/carp/ (last visited Oct. 2, 2010).

163 *Hubbard Broad., Inc.*, 777 F.2d at 396.

164 17 U.S.C. § 111(a)(3).

165 E. Microwave, Inc. v. Doubleday Sports, Inc., 691 F.2d 125, 130 (2d Cir. 1982).

166 17 U.S.C. § 512(a)(5) (2006).

167 *Id.* § 512(k)(1)(a).

all passive communications carriers (i.e., those that "do nothing but send a signal on"), regardless of the technology they employ, and regardless of whether they serve the sender or the receiver of the communication.[168] Carriers held to be entitled to the exemption include, for example, signal conduits that receive broadcast signals, convert them into microwave signals, and relay the converted signals via either satellite or terrestrial microwave repeater stations to cable systems.[169]

In addition to the pre-DMCA statutory precedent for exempting passive carriers from liability for copyright infringement, there is decisional precedent in cases involving conduit ISPs, including *Religious Technology Center v. Netcom On-Line Communication Services, Inc.*[170] *Netcom* was decided in 1995, three years before the DMCA was enacted. The holding in the case is that an Internet access provider that automatically and temporarily stores user-supplied material on its Usenet servers cannot reasonably be held liable for direct infringement because it "merely provides access to the Internet" and "does not create or control the content of the information available to its subscribers."[171] Reasoning that it would simply not be "workable" given the sheer volume of bits moving through their systems to hold ISPs liable for infringing copies generated automatically for temporary storage, the *Netcom* court emphasized the ISP's common carrier-like function:

> In a sense, a Usenet server that forwards all messages acts like a common carrier, passively retransmitting every message that gets sent through it. Netcom would seem no more liable than the phone company for carrying an infringing facsimile transmission or storing an infringing audio recording on its voice mail.[172]

Although the court was not entirely persuaded by Netcom's argument that it functioned as a proper common carrier,[173] the decision in the case ultimately turned on the passivity of Netcom's copying and its

168 *See* Infinity Broad. Corp. v. Kirkwood, 63 F. Supp. 2d 420, 425 (S.D.N.Y. 1999).

169 *See E. Microwave, Inc.*, 691 F.2d at 126.

170 Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 907 F. Supp. 1361 (N.D. Cal. 1995).

171 *Id.* at 1372.

172 *Id.* at 1369 n.12.

173 *See id.* ("Here, perhaps, the analogy is not completely appropriate as Netcom does more than just 'provide the wire and conduits.' Further, Internet providers are not natural monopolies that are bound to carry all the traffic that one wishes to pass through them, as with the usual common carrier.").

lack of control over the content transmitted.[174] As with the cases interpreting § 111, the fact that the provider seeking the exemption was not a common carrier per se didn't matter; the carrier's passivity in relation to the carried content was what mattered.

Revisiting the *Netcom* decision in light of the later-enacted DMCA, the Fourth Circuit in *CoStar Group, Inc. v. Loopnet, Inc.*[175] rejected the argument that *Netcom*'s holding of non-liability for passive copying by ISPs was supplanted by the DMCA's framework of affirmative defenses (i.e., the § 512 safe harbors).[176] The court held that Loopnet, a Web-hosting service that enabled its users to upload photos of commercial real estate, was entitled to rebut CoStar's case in chief by arguing that Loopnet's conduct in making RAM copies of photos uploaded by its users did not exhibit the element of volition necessary to establish copying for statutory purposes.[177] In concluding that Loopnet should not be considered an "actual duplicator" of the content uploaded by its users, the court relied on the oft-cited telephone company analogy: "Under such an arrangement, the ISP provides a system that automatically transmits users' material but is itself totally indifferent to the material's content. In this way, it functions as does a traditional telephone company when it transmits the contents of its users' conversations."[178]

Both the *Netcom* and the *CoStar* courts found it dispositive that the accused ISPs were acting only as conduits for information provided by their subscribers. The ISPs were indeed making copies of files uploaded by users, but they were doing so without knowledge of (or interest in) the contents of the files and with the sole aim of transmitting the contents from one subscriber to another. In other words, the copies were being made passively by the system without any element of control or volition on the part of the ISP. Without

174 *Id.* at 1372 (holding that "it does not make sense to adopt a rule that could lead to the liability of countless parties whose role in the infringement is nothing more than setting up and operating a system that is necessary for the functioning of the Internet").

175 CoStar Grp., Inc. v. Loopnet, Inc., 373 F.3d 544 (4th Cir. 2004).

176 *Id.* at 552.

177 *Id.* at 551 (concluding that "an ISP has not itself fixed a copy in its system of more than transitory duration when it provides an Internet hosting service to its subscribers"); *see also* Cartoon Network LP, LLLP v. CSC Holdings, Inc., 536 F.3d 121, 129 (2d Cir. 2008) (citing *CoStar* with approval and concluding that "the definition of 'fixed' imposes both an embodiment requirement and a duration requirement").

178 *CoStar Grp., Inc.*, 373 F.3d at 551.

control or volition, the courts held, there is no reasonable basis for a finding of direct liability.[179]

D. The Liability Implications of Intelligent Networks

Section 111 and § 512(a) of the Copyright Act together with *Netcom* and its progeny establish that intermediaries acting solely as passive carriers of content owned and controlled by others enjoy special treatment under copyright law. This special treatment, as Tim Wu has argued, is a key feature of a "de facto communications regime" that has developed within copyright law.[180] Before the rise of intelligent networks, conduit ISPs quite clearly qualified for special treatment as passive carriers, because all they did—like the phone company—was send other people's data on its way. Operators of intelligent broadband networks, by contrast, pride themselves on being more than "dumb pipes." In the shift from stupid to smart networks, which has entailed the deployment of packet-flow and packet-inspection technologies that enable broadband operators to both know and control what they're carrying for their subscribers, broadband operators risk forfeiting the protections from copyright liability to which they were entitled as passive carriers.

Arista Records LLC v. Usenet.com, Inc.,[181] a little-publicized district court case from 2009, may have important implications for broadband operators that make use of smart technologies within their systems. The defendant in the case, Usenet.com, was a Usenet host that offered subscribers access to 120,000 Usenet newsgroups for a monthly fee.[182] The plaintiffs were Arista Records and a handful of other major music distributors, who alleged that Usenet.com maintained a system that was overwhelmingly used for the purpose of

---

179 *Netcom On-Line Commc'n Servs., Inc.*, 907 F. Supp. at 1370 ("Although copyright is a strict liability statute, there should still be some element of volition or causation which is lacking where a defendant's system is merely used to create a copy by a third party."); *CoStar Grp., Inc.*, 373 F.3d at 550 (endorsing the reasoning in *Netcom* and holding that the Copyright Act "require[s] some aspect of volition and meaningful causation—as distinct from passive ownership and management of an electronic Internet facility"). The claim in *CoStar* was for direct infringement; the court left open the possibility that LoopNet's conduct, with additional facts, could be a basis for indirect liability. *Id.* at 551.

180 *See* Timothy Wu, *Copyright's Communications Policy*, 103 MICH. L. REV. 278, 279 (2004) (arguing that copyright law embodies both authorship policy and communications policy).

181 Arista Records LLC v. Usenet.com, Inc., 633 F. Supp. 2d 124 (S.D.N.Y. 2009).

182 *Id.* at 131.

illegally sharing copyrighted music files.[183] The claims in the case were for direct infringement of the right of distribution and secondary infringement of the rights of reproduction and distribution.[184]

In many ways, the facts of the case are reminiscent of those in *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd*.[185] Usenet.com's operators were not distributors of P2P software, but they did all of the things that the file sharing cases have specifically taught network intermediaries *not* to do if they want to escape secondary liability for the infringements of their users: they marketed themselves "as a safe alternative to peer-to-peer file sharing programs that were getting shut down"; they included the terms "warez" and "kazaa" in their Web site's metatags; they advertised "FREE MUSIC" and offered tutorials on how to download that used infringing files as illustrations.[186] Given that such actions patently give rise under *Grokster* to secondary liability based on an inducement theory of infringement, the court's decision that Usenet.com was secondarily liable for its users' infringements was altogether predictable.[187]

The more surprising aspect of the *Usenet.com* decision is the court's analysis of the plaintiffs' direct infringement claim, which culminated in a rejection of Usenet.com's argument that it should be shielded from liability for unauthorized distribution by *Netcom*'s exemption for passive carriers.[188] At least superficially, Usenet.com's reliance on *Netcom* was apt; both providers were Usenet hosts that temporarily stored files received from other Usenet hosts and automatically routed those files in real time to the users requesting them.[189] The Usenet system to which Usenet.com

183 *Id.* at 131–32.

184 *Id.* at 129. The plaintiffs specifically alleged direct infringement, inducement of infringement, contributory infringement, and vicarious infringement. *Id.*

185 *See* Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 936–37 (2005) (holding that "one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties").

186 *Usenet.com, Inc.*, 633 F. Supp. 2d at 132–33.

187 The Court in *Grokster* found that the record in the case was "replete with evidence that [the defendants] clearly voiced the objective that recipients use [their software] to download copyrighted works, and each took active steps to encourage infringement." *Grokster, Ltd.*, 545 U.S. at 923–24.

188 *Usenet.com, Inc.*, 633 F. Supp. 2d at 148 (rejecting defendants' reliance on *Netcom*).

189 *Id.* at 130–31 (describing Usenet.com as a Usenet provider and explaining how the Usenet functions to disseminate messages and files throughout the network and to

connected its users in 2009 was the same system, with the same underlying architecture, to which Netcom connected its users back in 1995. On summary judgment, Usenet.com argued that it acted, like Netcom, as a "common carrier" that delivers requested files to subscribers without active involvement.[190]

The court rejected the analogy, reasoning that unlike Netcom, which played no active role in selecting or managing the content flowing through its system, Usenet.com engaged in a number of forms of active network management: it blocked subscribers who posted spam; it throttled download speeds for subscribers who downloaded too much; and it took measures to restrict users from posting and downloading pornography.[191] It engaged in "automated filtering and human review, to remove access to certain categories of content, and to block certain users."[192] What it didn't do, even though it knew its service was being used to infringe copyrights, was use the technology at its disposal to block or attempt to block copyright infringing transfers.[193] The active steps Usenet.com took "transform[ed] Defendants from passive providers of a space in which infringing activities happened to occur [in]to active participants in the process of copyright infringement."[194] The court concluded that Usenet.com's network management activities satisfied the requirement of volitional conduct that was lacking in *Netcom*.[195] Therefore, unlike Netcom, which escaped liability for direct infringement because it did nothing to intervene in the flow of traffic across its system, Usenet.com was liable as a direct infringer of the plaintiffs' distribution right.

facilitate the sharing of content among users); Religious Tech. Ctr. v. Netcom On-line Commc'n Servs., Inc., 907 F. Supp. 1361, 1368 (N.D. Cal. 1995) (explaining that Netcom "maintain[s] a system whereby software automatically forwards messages received from subscribers onto the Usenet, and temporarily stores copies on its system").

190 *Usenet.com, Inc.*, 633 F. Supp. 2d at 148.

191 *Id.* at 157.

192 *Id.* at 148.

193 *Id.* at 153 (stating that although the defendants used "various tools and mechanisms" to block spam and limit download speeds, "they never used the same filtering capabilities to search for, limit or eliminate infringement on their service").

194 *Id.* at 149 (quoting Playboy Enters., Inc. v. Russ Hardenburgh, Inc., 982 F. Supp. 503, 513 (N.D. Ohio 1997)).

195 *But see* CoStar Grp., Inc. v. Loopnet, Inc., 373 F.3d 544, 556 (4th Cir. 2004) (holding that "[a]lthough LoopNet engages in volitional conduct to block photographs measured by two grossly defined criteria, this conduct, which takes only seconds, does not . . . add volition to LoopNet's involvement in storing the copy").

In theory, the same logic that barred Usenet.com from relying on *Netcom*'s exemption for passive carriers is applicable to broadband providers that use DPI and other smart network technology to manage the flow of traffic across their networks. Moreover, given that the DMCA safe harbor in § 512(a) incorporates a passive carriage requirement, conduit ISPs that have implemented packet inspection and filtering technologies within their networks—for reasons wholly unrelated to copyright enforcement—may find that they have dropped anchor in choppy waters if they have occasion to invoke the DMCA safe harbors in their defense.

The use of smart network technology impacts the availability to broadband providers of the defenses on which passive carriers are entitled to rely in actions for copyright infringement. The *Usenet.com* decision suggests, reasonably enough, that the benefits of traffic management and increased control over user content come with an obligation to assist in reducing infringement. It also suggests, reasonably enough, that the ability of a provider to filter for infringing content is becoming more germane to the analysis of intermediary liability as filtering technology improves. Jane Ginsburg considered this possibility in the wake of *Grokster*, given the Court's conclusion in the case that failure to filter, among other factors, is probative of a provider's intent to induce infringement.[196] The decision in *Usenet.com* supports Ginsburg's thesis that technological evolution may be in the process of readjusting the balance struck in the DMCA between copyright owners and service providers. The HEOA's requirement that college and university ISPs implement technology-based deterrents within their networks is further proof that a technology-driven reallocation of legal burdens is underway.[197]

It is worth remembering in this context that the *Netcom* court's decision was premised in part on the technical limitations to which ISPs were subject in 1995, when it was, in the words of the court, "practically impossible to screen out infringing bits from noninfringing bits."[198] We now live in a different state of the art;

196 *See* Jane C. Ginsburg, *Separating the Sony Sheep From the Grokster Goats: Reckoning the Future Business Plans of Copyright-Dependent Technology Entrepreneurs*, 50 ARIZ. L. REV. 577, 587 (2008) (positing that filtering may, in the wake of *Grokster*, afford a type of safe harbor from claims of inducement to infringe).

197 *See supra* note 15 and accompanying text.

198 Religious Tech. Ctr. v. Netcom On-line Commc'n Servs., Inc., 907 F. Supp. 1361, 1372–73 (N.D. Cal. 1995).

filtering technologies have been adopted by major online intermediaries, including YouTube[199] and Lime Wire,[200] whose users engage in a high volume of file and content sharing, much of it infringing. With the development of DPI, conduit ISPs from a technical standpoint are in a dramatically better position now than they were in 1995 to know and control the content they carry for their customers. While this is an alarming prospect for privacy advocates,[201] corporate rights owners view it as an opportunity. Moreover, broadband providers have strenuously resisted net neutrality regulation that would put *any* constraints on the uses to which they can put smart technology inside their networks. Considering the state of the art and the appetite of broadband providers for smarter networks and greater control over traffic, it is difficult to argue that today's conduit ISPs are not significantly better situated than their narrowband predecessors were to help prevent infringing uses of their services.

III

GRADUATED RESPONSE AND CONSUMER PROTECTION

As broadband providers venture outside the safety of § 512(a) and *Netcom* in the name of "reasonable network management," it is in their self-interest to explore increased cooperation with corporate rights owners in the war on piracy. Some ISPs have begun to do so under the umbrella of Arts+Labs, a collaborative that self-represents as a "partnership between technology companies and creators" that is

199 *See* Andy Greenberg, *YouTube's Filter Fails to Please*, FORBES.COM, Oct. 18, 2007, http://www.forbes.com/2007/10/18/google-viacom-video-tech-cx_ag_1018youtube.html.

200 *See The Lime Wire Beta Filtering System*, LIME WIRE, http://register.limewire.com/filter/ (last visited Oct. 2, 2010).

201 Consumer advocacy groups such as Free Press and the Center for Democracy & Technology oppose the use of DPI on privacy grounds. *See, e.g.*, *The Privacy Implications of Deep Packet Inspection: Testimony Before the Subcomm. on Commc'ns, Tech. and the Internet of the H. Comm. on Energy and Commerce*, 111th Cong. (2009) (statement of Leslie Harris, President and Chief Executive Officer, Center for Democracy & Technology), *available at* http://www.cdt.org/files/pdfs/20090423_dpi_testimony.pdf; M. CHRIS RILEY & BEN SCOTT, FREE PRESS, DEEP PACKET INSPECTION: THE END OF THE INTERNET AS WE KNOW IT? (2009), *available at* http://www.freepress.net/files/Deep_Packet_Inspection_The_End_of_the_Internet_As_We_Know_It.pdf. Privacy-conscious users can defeat DPI, however, by encrypting their file transfers. Bridy, *supra* note 8, at 595–96. According to some estimates, 20% of BitTorrent traffic is already encrypted. *See* Brad Reed, *Could Traffic Filtering Get AT&T Into Trouble?*, PC WORLD, Jan. 18, 2008, http://www.pcworld.com/businesscenter/article/141520/could_traffic_filtering_get_atandt_into_trouble.html.

dedicated to educating consumers about the dangers of "*net pollution*—spam, malware, computer viruses and illegal file trafficking."[202] In comments before the FCC in the Open Internet NPRM, Arts+Labs echoed the MPAA's call for government nonintervention in the private ordering of online copyright enforcement: "Content creators should be able to work with any other Internet participant on enhancements that enable them to directly combat digital theft and to better compete with Internet piracy by offering higher quality, safety, and reliability."[203] "Enhancements" of this nature are expressly contemplated in § 512(i), which defines "standard technical measures" to combat infringement in terms of "a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process."[204] How privately implemented enforcement measures might ultimately affect consumers, however, must be weighed carefully and managed prudently, particularly given that consumers have no place at the table when it comes to negotiations between broadband providers and rights owners about how best to "combat digital theft." This Part of the Article proposes a number of principles to guide private ordering in the arena of online copyright enforcement so that the interests of consumers are not shortchanged.

A. The Impact of Disconnection

In some countries in the European Union, universal access to broadband is regarded as a basic right.[205] This is not the case in the United States, but Congress in 2009 appropriated $4.7 billion in economic stimulus funds to enhance the U.S. broadband infrastructure

[202] *About Us*, ARTS+LABS, http://www.artsandlabs.com/about_us/About_Us.aspx (last visited Oct. 2, 2010). Members of the collaborative include AT&T, Verizon, Viacom, NBC Universal, Microsoft, BMI, ASCAP, and the Songwriters Guild of America. *Id.*

[203] *Comments of Arts+Labs in the Matter of Preserving the Open Internet Broadband Industry Practices: Before the Fed. Commc'ns Comm'n*, GN Docket No. 09-191 (2010).

[204] 17 U.S.C. § 512(i)(2)(A) (2006).

[205] Finland was the first country in the world to create a legal right to broadband Internet access. *See* Saeed Ahmed, *Fast Internet Access Becomes a Legal Right in Finland*, CNN, Oct. 15, 2009, http://www.cnn.com/2009/TECH/10/15/finland.internet.rights/index.html. Spain soon followed. *See Spain Makes Broadband a Universal Right*, CBC NEWS, Nov. 18, 2009, http://www.cbc.ca/technology/story/2009/11/18/spain-universal-broadband-access.html.

and expand access to unserved populations.[206] This substantial public investment in broadband uptake recognizes the critical role the Internet now plays in contemporary American life and the extent to which the public and the economy have come to rely on uninterrupted connectivity. Taking this reliance into account, termination of Internet access represents a powerful and far-reaching sanction that directly impacts not only the ability of Internet users to consume media but also their ability to work, learn, communicate, manage finances, and participate in the collective life of society. Even a temporary suspension of access can represent a hardship, particularly considering that a whole household stands to lose access under a graduated response regime as a result of a single member's supposed copyright infringements. In light of these factors, privately implemented graduated response regimes should be designed to minimize the likelihood of mistaken responses, to maximize opportunities for consumer compliance before the imposition of any sanction, and to limit the duration of any access-related sanction imposed in the absence of a neutral adjudication of infringement.

B. Opportunity to Contest Notices

Users should be given an opportunity to contest notices of infringement with their ISPs as the notices are received and before any sanction is imposed. When the music industry first began suing individual file sharers, it pursued a number of well-publicized cases of mistaken identity, about which its representatives were glibly unapologetic: if they dragged some innocent people into court along with the guilty ones, they said, that was the cost of making a good point.[207] The problem of false positives in online copyright surveillance, whether that surveillance is being carried out by human agents or automated crawlers, is well documented[208] and has

[206] *See* U.S. Dep't of Commerce, Nat'l Telecomms. & Info. Admin., *Broadband Technology Opportunities Program (BTOP)*, BROADBAND USA: CONNECTING AMERICA'S COMMUNITIES, http://www2.ntia.doc.gov/ (last visited Oct. 2, 2010).

[207] *See* Dennis Roddy, *The Song Remains the Same*, PITTSBURGH POST GAZETTE, Sept. 14, 2003, http://www.post-gazette.com/columnists/20030914edroddy0914p1.asp.

[208] *See, e.g.*, DANIEL CASTRO ET AL., THE INFO. TECH. & INNOVATION FOUND., STEAL THESE POLICIES: STRATEGIES FOR REDUCING DIGITAL PIRACY 10 (2009) (advocating filtering but conceding that "content recognition systems are not perfect"); MICHAEL PIATEK ET AL., CHALLENGES AND DIRECTIONS FOR MONITORING P2P FILE SHARING NETWORKS—OR—WHY MY PRINTER RECEIVED A DMCA TAKEDOWN NOTICE 1 (2008) (stating that "it is possible for a malicious user (or buggy software) to implicate (frame) seemingly any network endpoint in the sharing of copyrighted materials"); Yu, *supra* note

undermined public confidence in both the methods and the good faith of corporate rights owners. In the project of online surveillance, rights owners have historically put zeal before accuracy. If broadband operators agree to adopt graduated response protocols, especially if those protocols involve ISP-based filtering of material identified as copyright infringing, that order of priority must be reversed. To that end, the technologies on which ISPs rely to block infringing file transfers should be mature and thoroughly tested before they are deployed.[209] Whether—and, if so, how—such technologies can be calibrated to recognize fair uses of copyrighted content remain vexing questions that proponents of filtering, to their discredit, tend to ignore.[210] Assuming that false positives will occur, even in the most sophisticated digital fingerprinting or watermarking systems, broadband providers should provide subscribers with an efficient, accessible, and responsive process for contesting the notices of infringement they receive—something akin to the counter-notice and put-back provisions in § 512(g) of the DMCA.[211]

C. Correspondence of Notices to "Strikes"

When it comes to adding up strikes, ISPs should count a single notice of infringement that alleges multiple instances of infringement as only one "strike" against the subscriber receiving the notice. To do otherwise would effectively take the "graduated" out of graduated response and would undermine the rehabilitative principle that

10, at 15 (asserting that "infringement-identifying technology has been fairly unreliable thus far").

[209] Opponents of filtering question whether the technology will ever be sophisticated enough and argue that it is doomed to be both overinclusive and underinclusive in its blocking. *See, e.g.*, MEHAN JAYASURIYA ET AL., PUBLIC KNOWLEDGE, FORCING THE NET THROUGH A SIEVE: WHY COPYRIGHT FILTERING IS NOT A VIABLE SOLUTION FOR U.S. ISPS (2009), *available at* http://www.publicknowledge.org/pdf/pk-filtering-whitepaper-200907.pdf.

[210] As an example, BayTSP, which has successfully marketed its Content Authentication Platform to major movie studios, music labels, and sports leagues, touts the accuracy of its system, but it makes no mention of protecting fair uses of copyrighted digital content. *See BayTSP Announces 15 Customers Using its Content Authentication Platform for Copyright*, ALL BUSINESS (Mar. 2, 2009), http://www.allbusiness.com/media-telecommunications/movies-sound-recording/11799800-1.html (announcing that fifteen companies are using BayTSP's Content Authentication Platform and describing the underlying technologies as "best of breed").

[211] *See* 17 U.S.C. § 512(g)(3) (2006) (setting forth the means by which recipients of notices of infringement can counter the allegations therein and request restoration of blocked content).

infringing consumers should be given repeated opportunities to reform and comply. In the context of § 512(i), rights owners have advocated a definition of "repeat infringer" that would require termination of access for a user who has received only two notices of infringement, if the first notice alleged multiple infringements.[212] The position is overly aggressive, given the margin of error involved in precisely identifying infringers[213] and the fact that notices of infringement generated by rights owners are only red flags of infringement and not legal judgments.[214] While corporate rights owners have shown little inclination to recognize the important difference between an accusation and a judgment when it comes to online infringement, ISPs have service obligations to their subscribers that require them to be more circumspect. If, as representatives of notice-forwarding ISPs have said, repeat notices to the same user are seldom required to secure compliance,[215] then counting one notice as no-more-than-one strike will not meaningfully compromise deterrence.

D. Graduation of Sanctions

The principle underlying graduated response is that sanctions should escalate as infractions accrete. The disciplinary approach is an incremental one, and in the interest of consumer protection, there should be more, rather than fewer, increments when it comes to the nature and duration of access-related sanctions. To maximize opportunities for Internet users to comply, ISPs that agree to implement a graduated response regime should graduate the access-

212 *See* UMG Recordings, Inc. v. Veoh Networks Inc., 665 F. Supp. 2d 1099, 1116–18 (C.D. Cal. 2009).

213 Online surveillance of P2P networks results only in the identification of IP addresses involved in the sharing of copyrighted files, not in the identification of the individuals sharing those files. Because IP addresses are sometimes dynamically assigned, and because more than one person can connect to the Internet from a single, fixed IP address, it is inaccurate to assert a one-to-one correspondence between an IP address and an infringer.

214 *See* Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090, 1105 (W.D. Wash. 2004) (pointing out that notices from rights owners could be erroneous and do not, on their own, provide evidence of blatant copyright infringement).

215 *See* David Carnoy, *Verizon Ends Service of Alleged Illegal Downloaders*, CNET NEWS, Jan. 20, 2010, http://news.cnet.com/8301-1023_3-10437176-93.html?tag=news LeadStoriesArea.1 ("[The Verizon representative] also noted that . . . issuing warning letters is proving to be effective."); Greg Sandoval, *AT&T Exec: ISP Will Never Terminate Service on RIAA's Word*, CNET NEWS, Mar. 25, 2009, http://news.cnet.com/8301-1023 _3-10204514-93.html ("[An AT&T vice president] said the notices worked. The company saw very few repeat offenders.").

related sanctions they impose, beginning with a speed sanction after three uncontested notices and graduating to a brief suspension of access with the fourth. Because false positives are likely, and innocents often co-connect with infringers, ISPs should refrain from imposing access-related sanctions of any significant duration (e.g., more than a few days) absent a neutral adjudication of infringement obtained by a copyright owner. For cases involving truly persistent or high-volume infringers, rights owners have, as they have always had, recourse to courts of law. In such cases, they should continue to vindicate their rights judicially and should not look to graduated response as a panacea.

Not all ISPs are going to be amenable to imposing access-related sanctions without a court order. While Comcast and Verizon reserve the right in their terms of service to make unilateral judgments about account terminations in cases involving copyright infringement,[216] AT&T has said publicly that the company will not suspend or terminate any user's access without a court order.[217] From the point of view of DMCA compliance, the insistence on a court order is defensible in light of the ambiguity that lingers around the definition of "repeat infringer."[218] How and to what extent providers that reserve the right to make their own judgments about infringing activity are exercising their discretion is difficult to know.

For ISPs that are inclined to impose access-related sanctions based solely on notices of infringement (i.e., without a court order), the efficacy of short suspensions should be tested empirically before sanctions of longer duration are considered. The goal should be to identify and implement the minimum sanction necessary to achieve broad-based compliance. If graduated response works, as rights owners seem confident it will, there will be few cases that actually test what it means to be "out" after three strikes. The cases on the margin should be treated as candidates for full adjudication on the merits.

---

[216] *See supra* note 97 and accompanying text.

[217] *See* Sandoval, *supra* note 215 (quoting Jim Cicconi, a senior executive vice president at AT&T).

[218] *See supra* notes 43 and 59 and accompanying text.

E. Disclosure of Enforcement Practices

Broadband providers should provide full disclosure of their copyright enforcement practices to prospective and existing customers, including whether they use packet inspection or other intrusive technology for copyright enforcement purposes. The Open Internet NPRM requires providers of broadband Internet access to "disclose such information concerning network management and other practices as is reasonably required for users and content, application, and service providers to enjoy the protections" secured by the proposed rules.[219] This transparency requirement, vague as it is, has its roots in the Comcast torrent-throttling episode.[220] Rather than disclosing to users that it was blocking P2P traffic to control network congestion, Comcast actively concealed its activities from the affected users by sending fake error messages.[221] The messages made it appear as if the transfers were failing for reasons outside of Comcast's control.[222]

On the heels of the Comcast incident, researchers conducting a study in early 2008 observed thousands of incidents in which BitTorrent uploads were being blocked by ISPs.[223] At the time, the ISPs responsible for most of the blocking had not publicly disclosed their network management practices.[224] If the network management practices in which ISPs engage are truly justified and reasonable, as ISPs contend, then there is no legitimate reason *not* to disclose them. Moreover, users have a right to know how broadband networks are being managed if management practices materially impact their online experience, including their ability to engage in high-speed file transfers using P2P protocols.

In terms of copyright enforcement disclosures, the DMCA has long conditioned the availability of its safe harbors on ISPs' adopting and publishing policies that provide for termination of subscribers who

---

219 Preserving the Open Internet, Broadband Industry Practices, 74 Fed. Reg. 62638, 62662 (proposed Nov. 30, 2009) (to be codified at 47 C.F.R. pt. 8).

220 *See* Bridy, *supra* note 8, at 598–99; *see also* Preserving the Open Internet, Broadband Industry Practices, 74 Fed. Reg. at 62648 (referring to the Comcast episode as an instance of a service provider "concealing information that consumers would consider relevant in choosing a service provider or a particular service option").

221 Bridy, *supra* note 8, at 598–99.

222 *See id.*

223 Preserving the Open Internet, Broadband Industry Practices, 74 Fed. Reg. at 62648.

224 *Id.*

are repeat infringers.[225] The language of these policies tends to track the language of the statute very closely and provides little if any detail about actual implementation.[226] If a broadband provider agrees to engage in graduated response and/or filtering on behalf of rights owners, that provider should so disclose in its terms of service. The disclosure should be affirmative and not merely couched in terms of a reservation of rights. Comcast's current terms of use, for example, expressly reserve the right "to monitor bandwidth, usage, transmissions, and content" and take remedial actions including "temporary or permanent removal of content, . . . filtering of Internet transmissions, and the immediate suspension or termination of all or any portion of the Service."[227] Cox reserves the right in its subscriber agreement to "monitor . . . any content . . . in Cox's possession . . . as Cox deems necessary to satisfy any applicable law" and the right to engage in "protocol filtering."[228] Verizon reserves the right to "block or remove any unlawful content [that users] . . . transmit to or from any Verizon server."[229] Each of these reservations of rights is drafted so broadly that any one of these providers could begin filtering for rights owners tomorrow without revising the existing language or providing any additional notice to subscribers. In the interest of transparency, broadband providers should be more forthright about their copyright enforcement policies—telling users not what they might do, but what they actually do.

CONCLUSION

When Congress passed the DMCA in 1998, it did so with the stated goal of "preserv[ing] strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment."[230] Although the DMCA did not make monitoring for infringing content a condition of any ISP's eligibility for safe harbor, the legislative history is clear that the creation of safe harbors was

225 17 U.S.C. § 512(i)(1)(A) (2006).

226 *See supra* note 97 and sources cited therein (quoting ISP terms of service and acceptable use policies).

227 *Comcast Acceptable Use Policy*, *supra* note 97.

228 *Cox Communications Subscriber Agreement*, *supra* note 111.

229 *Verizon Terms of Service*, *supra* note 97.

230 H.R. REP. NO. 105-796, at 72 (1998).

"not intended to discourage the service provider from monitoring its service for infringing material."[231] Inasmuch as the DMCA was designed to promote interindustry cooperation between rights owners and ISPs, the seeds of graduated response were sown more than a decade ago, before the broadband revolution and well before the development of smart network technologies like DPI. The government's 2010 Joint Strategic Plan on Intellectual Property Enforcement expresses continuing official support for interindustry cooperation in online copyright enforcement, particularly with respect to the phenomenon of repeat infringement.[232]

As filtering technologies have become more sophisticated, and as ISPs have implemented them for reasons unrelated to copyright enforcement, the groundwork has been laid—though perhaps only accidentally—for a private reallocation of online copyright enforcement burdens. The FCC, even if it acts to reclassify the connectivity component of broadband as a Title II telecommunications service, is unlikely to intervene in the name of net neutrality to prevent this private (re)ordering by, for example, prohibiting content blocking or filtering by ISPs. If that turns out to be the case, ISPs and rights owners must take it upon themselves, in the interest of the customers they aim to get and keep, to ensure that their private arrangements for enforcing copyrights online are both adequately transparent and meaningfully consumer-protective.[233]

---

[231] *Id.* at 73.

[232] *See* OFFICE OF THE U.S. INTELLECTUAL PROP. ENFORCEMENT COORDINATOR, 2010 JOINT STRATEGIC PLAN ON INTELLECTUAL PROPERTY ENFORCEMENT 17 (2010), *available at* http://www.whitehouse.gov/omb/assets/intellectualproperty/intellectual property_strategic_plan.pdf ("The Administration believes that it is essential for the private sector, including content owners, Internet service providers, advertising brokers, payment processors and search engines, to work collaboratively . . . to seek practical and efficient solutions to address infringement. . . . Specifically, the Administration encourages actions by the private sector to effectively address repeated acts of infringement, while preserving the norms of legitimate competition, free speech, fair process and the privacy of users.").

[233] It is significant in this regard that the Joint Strategic Plan, *id.*, even as it encourages greater cooperation between ISPs and rights owners to address repeat infringement, cites the need to protect the norms of privacy, fairness, and free expression.