Harvard Journal of Law & Technology
Volume 27, Number 1 Fall 2013

STANDARDS FOR DETERMINING WHEN ISPS HAVE FALLEN OUT OF SECTION 512(A)

*Nathan Lovejoy**

TABLE OF CONTENTS

I. INTRODUCTION

For over a decade, the record industry has been in a state of upheaval. Revenues have steadily declined,[1] businesses have experi-

* Harvard Law School, J.D. 2013. Many thanks to Terry Fisher, Zach Lerner, Craig Fratrik and the JOLT editors for guiding this Note along its path.

1. *See*, *e.g.*, 2008 Year-End Shipment Statistics, RIAA, http://76.74.24.142/1D212C0E-408B-F730-65A0-C0F5871C369D.pdf (showing a decline in revenue for all but one year between 1999 and 2008).

mented (both successfully and unsuccessfully) with new ways of delivering music,[2] and listeners have shifted the way they spend money on entertainment.[3] Some observers have identified the rise of file-sharing networks as a key inflection point in accelerating the declines in revenue.[4] Others have cited the shift from albums to singles as the primary unit of music sales as the cause of the industry's woes.[5] Reliance on either explanation requires the assumption of expanding broadband access and the development of new methods of consumption through the Internet. In large part, the reconfiguration of the record industry can be correlated with the growth in high-speed Internet connections, with more people connecting and service bandwidth increasing each year.[6] The better the quality of the connection and the larger the connected user-base, the more opportunity there is for infringing and noninfringing businesses alike. Amidst the maelstrom of copyright infringement occurring online, however, Internet service providers ("ISPs") have remained protected from liability despite providing the necessary physical prerequisites and the basic tools that enable this activity. This is thanks to 17 U.S.C. § 512(a).

Section 512(a) provides a safe harbor from liability for ISPs, provided that they operate their networks within certain statutory bounds, generally requiring the transmission of third-party information without interference, modification, storage, or selection.[7] It, along with the other safe harbors in section 512, came as a result of intense negotiations among Congress, content creators, ISPs, and online distributors in the mid- to late-1990s that led to the passage of the Digital Millennium Copyright Act ("DMCA") in 1998.[8] The legislative effort was in response to both a growing concern over copyright infringement

---

2. For an example of the unsuccessful, see Robin Wauters, *SpiralFrog Goes Belly Up*, TECHCRUNCH (Mar. 20, 2009), http://techcrunch.com/2009/03/20/spiralfrog-goes-belly-up/; for an example of the comparatively more successful, see Greg Sandoval, *Spotify Tops 1 Million Paid U.S. Subscribers in One Year*, CNET (Dec. 6, 2012, 9:39 AM), http://news.cnet.com/8301-1023_3-57557566-93/spotify-tops-1-million-paid-u.s-subscribers-in-one-year/.

3. *See* Will Page, *Wallet Share*, 22 ECON. INSIGHT, Apr. 18, 2011, at 1, 3, *available at* http://prsformusic.com/creators/news/research/Documents/Economic%20Insight%2022%20Wallet%20Share.pdf (describing the changing proportion of spending on live music in the UK as compared to recorded music).

4. *See, e.g.*, Bennett Lincoff, *Common Sense, Accommodation and Sound Policy for the Digital Music Marketplace*, 2 J. INT'L MEDIA & ENT. L. 1, 4–5 (2008) (linking the degree of downloads via file-sharing services with the decline in record label revenue).

5. *See generally* Anita Elberse, *Bye-Bye Bundles: The Unbundling of Music in Digital Channels*, 74 J. MARKETING, May 2010, at 107, 108 (finding a correlation between revenue declines and the sale of digital singles as opposed to physical albums).

6. *See* ITU, *The World in 2011: ICT Facts and Figures*, ITU TELECOM WORLD 2011, *available at* http://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2011.pdf.

7. 17 U.S.C. § 512(a), (k) (2012).

8. *See* David L. Hayes, *Copyright Liability of Online Service Providers: Part II*, 19 THE COMPUTER & INTERNET LAWYER, Nov. 2002, at 15, 21–22.

online and the potential for copyright liability to hamper the development of networked connectivity and online businesses.[9] Arguably, it has been the DMCA's safe harbors that have enabled much of the vibrancy that we see in the online world today.[10]

Yet, the technological hurdles for enforcement ISPs face today are different — and possibly lower — than those of the 1990s,[11] while the pattern of copyright infringement has continued to grow. This has led to efforts by rights holders to seek supplementary means of suppressing infringement.[12] There have been a number of efforts in this direction, with varying degrees of success,[13] that have also, at times, encountered substantial public resistance. The outcry over, and subsequent failure of, major reform legislation in early 2012[14] exemplified the potential strength of such resistance.

Increasingly, efforts to stem infringement have focused on bringing ISPs into the picture.[15] ISPs' cautious amenability to this approach perhaps represents a willingness to play a more active role in combatting copyright infringement. It also may reflect the change in what has become technologically possible for ISPs in the years since the passage of the DMCA. If ISP-centric efforts to combat infringement ramp up over time, there is a danger that ISPs could gradually whittle away at the very qualities that guarantee them protection within the section 512(a) safe harbor, ironically exposing them to greater risk of liability for the very infringements they may seek to prevent. However, the point at which these policing efforts constitute sufficient interference to cause ISPs to fall out of the protection of the section 512(a) safe harbor remains largely unexplored.

Section 512(a) has been such a powerful safe harbor that the familiar narrative is of a service provider trying to define itself in such a way as to gain its protection, but then failing to meet its require-

---

9. *See* 3 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 12B.01[C][1] (2006) ("On the one hand . . . 'copyright owners will hesitate to make their works readily available on the Internet,' . . . on the other hand, having a profusion of copyrighted works available will not serve anyone's interest if the Internet's backbone and infrastructure are sued out of existence.").

10. *See, e.g.*, David Kravets, *10 Years Later, Misunderstood DMCA Is the Law That Saved the Web*, WIRED (Oct. 27, 2008, 3:01 PM), http://www.wired.com/threatlevel/2008/10/ten-years-later/.

11. *See* Annemarie Bridy, *Graduated Response and the Turn to Private Ordering in Online Copyright Enforcement*, 89 OR. L. REV. 81, 123–24 (2010) [hereinafter *Private Ordering*] (noting the changing technological environment).

12. *See infra* Part III.

13. *See infra* Part III.A.

14. *See* Bill D. Herman, *A Political History of DRM and Related Copyright Debates, 1987–2012*, 14 YALE J.L. & TECH. 162, 214–23 (2012) (reviewing the SOPA/PIPA debates).

15. *See infra* Part III.B.

ments.[16] In practice, courts have strictly limited section 512(a) protection to a small group of entities that provide the physical transmission media for the Internet.[17] As the ISPs within this core become ever more active in managing their networks, however the question will shift from what gets you *in* to section 512(a) to what pushes you out.

This paper outlines the environment in which the possibility of losing section 512(a) protection has grown more likely and notes three potential standards courts could use to determine whether loss of protection is warranted. Part II provides a background to the section 512(a) safe harbor and its requirements, as well as the influence the *Religious Technology Center v. Netcom*[18] decision may have had on its formation. Part III highlights past, current, and potential means of policing copyright infringement online with an emphasis on those methods available to ISPs. Part IV compares three potential standards that could delineate the boundaries of section 512(a)'s protection: a neutrality standard, a knowledge-based standard, and a categorical conduit/editorial standard. Part V concludes.

II. SECTION 512(A) & (K): BACKGROUND & REQUIREMENTS

It is first necessary to examine the statutory language constituting the section 512(a) safe harbor and its origin. Section 512(a) was intended to "protect qualifying service providers from liability for all monetary relief for direct, vicarious and contributory infringement,"[19] for activities that fall within a specified range performed by entities that meet the criteria of section 512(k)(1)(A).

A. Section 512(a) Activity Requirements

The section 512(a) provision defines the activities for which service providers will not be held liable, namely "transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or . . . the intermediate and transient storage of that material . . . ."[20] For instance, an ISP could call upon this provision to protect itself from liability for

16. *See, e.g.*, A&M Records, Inc. v. Napster, Inc., No. C 99-05183 MHP, 2000 WL 573136 (N.D. Cal. May 12, 2000).

17. A primary example has been the exclusion of file-sharing networks from section 512(a) eligibility. *See, e.g.*, *In re* Aimster Copyright Litig., 252 F. Supp. 2d 634, 659 (N.D. Ill. 2002), *aff'd*, 334 F.3d 643 (7th Cir. 2003). *See also* Jennifer Bretan, Note, *Harboring Doubts About the Efficacy of § 512 Immunity Under the DMCA*, 18 BERKELEY TECH. L.J. 43, 48–49 (2003) (describing the narrowing of the section 512(a) safe harbor).

18. 907 F. Supp. 1361 (N.D. Cal. 1995).

19. H.R. REP. NO. 105-796, at 73 (1998) (Conf. Rep.).

20. 17 U.S.C. § 512(a) (2012).

merely routing packets through their network, which, together, constitute an infringing music download — despite providing the connections and transmission necessary for that transaction to occur.

This safe harbor is conditioned on the service provider acting in a specified manner with regard to that activity, enumerated by sections 512(a)(1)–(5). Subsection (1) requires that the transmission "was initiated by or at the direction of a person other than the service provider,"[21] preventing the use of the safe harbor to shield infringement carried out at the volition of the service provider itself. Subsection (2) requires that transmissions occur as a result of "an automatic technical process without selection of the material by the service provider . . . ."[22] According to the legislative history, this condition was meant to keep "editorial function[s]" of service providers open to liability for infringement, while protecting mere responses to requests.[23] Subsection (3) stipulates that the service provider must not "select the recipients of the material except as an automatic response to the request of another person,"[24] further underscoring the exclusion of editorial or volitional conduct by the service provider. Subsection (4) says that service providers cannot make use of the safe harbor for material stored by them in a "manner ordinarily accessible to anyone other than anticipated recipients" or for a time longer than "reasonably necessary" for transmission.[25] The House Report notes that neither access to stored material by third parties, through activities like illegal intrusion and maintenance, nor access by law enforcement would break the safe harbor,[26] but subsection (4) serves to distinguish traditional ISP activities from online services like YouTube, which store material for general availability.[27] Finally, subsection (5) requires that the service provider provide transmission "without modification of its content."[28] According to the House Report, the nonmodification requirement is not as broad as it may seem at first. It notes that the concern is with "content" defined so as to exclude "form" and gives as an example the transmission of an email without the sender's intended bold or italic formatting as a permissible modification of form but not content.[29]

In all, the requirements of section 512(a)(1)–(5) generally serve to protect activities that are traditionally in the purview of common car-

21. *Id.* § 512(a)(1).
22. *Id.* § 512(a)(2).
23. H.R. REP. NO. 105-551, pt. 2, at 51 (1998).
24. 17 U.S.C. § 512(a)(3).
25. *Id.* § 512(a)(4).
26. H.R. REP. NO. 105-551, pt. 2, at 51.
27. These types of services will generally be able to look to the section 512(c) safe harbor for protection, but are not discussed here.
28. 17 U.S.C. § 512(a)(5).
29. H.R. REP. NO. 105-551, pt. 2, at 51.

riers — providing service to customers on an automatic, nondiscriminatory basis.[30] It also distinguishes (though not explicitly) between conduct occurring at the volition of the service providers and conduct occurring at the volition of their customers, breaking the safe harbor the moment the former intrudes upon the latter.[31]

B. Section 512(k)(1)(A) Service Provider Requirements

The protections for service providers under section 512(a) are strong and ISPs have fought to define themselves so as to fit within the statute's bounds. However the statute limits the type of entity that can avail itself of these protections.[32] Where section 512(a) protects a set of *activities*, section 512(k)(1)(A) limits the type of service provider who can take advantage of those limited set of activities.

The definition of "service provider" in section 512(k)(1)(A) incorporates much of the transaction-specific requirements of sections 512(a)(1)–(5), defining a service provider as "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."[33] The language of sections 512(a)(1), (2), and (5) imply both that the volition of the third-party/customer must remain paramount and that the taking on of an editorial role breaks the safe harbor. The core function of section 512(k)(1)(A) is to limit section 512(a) protections to entities that engage in traditional, common carrier-like data services in their normal course of business. Section 512(a) thus does not apply to entities that may engage in common carrier-like data service only incidentally, activities that do not qualify as "digital online communications," or actions that more closely resemble those of publishers, which fall under section 512(c).[34]

Given the overlap of sections 512(a) and (k) in their requirements, it may be difficult to tease out which anti-infringement measures go

30. *See* Eric Evans, *From the Cluetrain to the Panopticon: ISP Activity Characterization and Control of Internet Communications*, 10 MICH. TELECOMM. & TECH. L. REV. 445, 463 (2004). *See also* H.R. REP. NO. 105-551, pt. 2, at 63 (describing how this set of activities was drawn from the "conduit-only functions" that are covered by the definition of "telecommunications" in the Communications Act, an area historically near the core of the common carrier set).

31. Indeed, some courts have explicitly recognized this connection between a volition requirement and ISP liability generally. *See, e.g.*, CoStar Grp., Inc. v. LoopNet, Inc., 373 F.3d 544, 550 (4th Cir. 2004).

32. 17 U.S.C. § 512(k)(1)(A).

33. *Id.*

34. Indeed, in her analysis of the history of the DMCA safe harbors, Annemarie Bridy finds the publisher/conduit distinction particularly relevant. *Private Ordering*, *supra* note 11, at 89.

so far as to push ISPs out of the definition of service provider altogether and which merely bar protection for infringement conducted under the influence of that measure. The distinction between abandoning definitional precursors for protection and engaging in instances of unprotected activity is critical. Moving out of the section 512(k)(1)(A) zone would remove section 512(a) protection for *all* of an ISP's activities rather than the specific transmissions that do not fit section 512(a) criteria. Because they tend to paint very similar pictures, however, the analysis of falling out of either definitional boundary is the same.

C. Section 512(i) Conditions

ISPs looking to take advantage of the section 512(a) safe harbor must meet two other requirements that are pertinent to this discussion: the conditions in section 512(i) that require implementing a termination policy for repeat infringers and accommodating standard technical measures combatting infringement.[35] Section 512(i)(1)(A) requires that a service provider "reasonably implement[], and inform[]" its users of a termination policy for repeat infringers.[36] This condition, however, does not go so far as to require investigation of all potential infringement.[37] Section 512(i)(1)(B), which requires the accommodation of "standard technical measures," was a reflection of Congress' attempt to establish a balance between its faith that technological developments would help resolve the problem of online infringement and its desire only to require technologies that have achieved a broad, industry-wide consensus.[38]

D. Unclear Influence of Netcom

Before the introduction of the DMCA and the section 512 safe harbors, courts had developed divergent approaches to ISP liability for copyright infringement by their users. *Playboy Enterprises, Inc. v. Frena*[39] and *Religious Technology Center v. Netcom*[40] typified the two main approaches.[41]

---

35. 17 U.S.C. § 512(i)(1)(A)–(B).

36. *Id.* § 512(i)(1)(A).

37. *See, e.g.*, Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1114 (9th Cir. 2007) (discussing the lack of a requirement to investigate all potential infringement within the context of the narrower section 512(c) safe harbor). *See also* H.R. REP. NO. 105-551, pt. 2, at 61 (1998).

38. H.R. REP. NO. 105-551, pt. 2, at 61–62.

39. 839 F. Supp. 1552, 1557–59 (M.D. Fla. 1993).

40. 907 F. Supp. 1361, 1372 (N.D. Cal. 1995).

41. *Compare* Playboy Enters., Inc. v. Webbworld, Inc., 991 F. Supp. 543, 551 (N.D. Tex. 1997), *aff'd*, 168 F.3d 486 (5th Cir. 1999) (employing the *Frena* approach) *with* Marobie-

Frena involved a bulletin board system ("BBS") provider that allowed its users to store images on its network, where other users could then download them.[42] After discovering some of its photos on the system, Playboy sued the BBS operator for copyright infringement.[43] The court held that the creation of copies by a service provider, even without intent to infringe, was enough to satisfy the requirements for copyright infringement on a direct, rather than secondary, theory.[44] In contrast, *Netcom* crafted a buffer of protection for ISPs whose users were engaged in copyright infringement.[45] In that case, Religious Technology Center (RTC) sued an ex-Scientology minister for posting portions of the works of L. Ron Hubbard on a Usenet newsgroup, to which he gained access through a BBS, and which in turn was provided access to the Internet by Netcom.[46] After failing to convince the latter two entities to take corrective action, RTC included them as defendants in the suit for copyright infringement.[47] Unlike in *Frena*, however, the court held that Netcom could not be held directly liable for the automatic functioning of its system.[48] However, it left open the possibility of secondary liability if Netcom knew of the infringement, had the ability to prevent it, and failed to do so.[49] The court specifically made note of the fact that Netcom "does not completely relinquish control over how its system is used," and as a result, it would be "fair . . . to hold Netcom liable for contributory infringement where" it has knowledge and ability to prevent the infringement through simple measures.[50] By extension, it would seem that had Netcom operated in an entirely hands-off manner, its exposure to contributory liability would have been substantially reduced.

There is evidence that the section 512(a) safe harbor was modeled after *Netcom*. The Senate Judiciary Committee report on a draft of the DMCA cited both *Netcom* and *Frena* in a discussion of the current state of the law before proceeding to describe its approach of creating safe harbors along the lines of *Netcom* and invalidating the *Frena* approach.[51] Indeed, some courts[52] and commentators[53] have suggested

---

FL, Inc. v. Nat'l Ass'n of Fire Equip. Distribs., 983 F. Supp. 1167, 1178 (N.D. Ill. 1997) (employing *Netcom*).

42. *Frena*, 839 F. Supp. at 1554.

43. *Id.*

44. *Id.* at 1559.

45. *Netcom*, 907 F. Supp. at 1368–69.

46. *Id.* at 1365–66.

47. *Id.* at 1366.

48. *Id.* at 1372–73.

49. *Id*. at 1373–75.

50. *Id.* at 1375.

51. S. REP. NO. 105-190, at 19 n.20 (1998).

52. *See, e.g.*, Ellison v. Robertson, 357 F.3d 1072, 1081 (9th Cir. 2004) (affirming the district court's determination that "Congress intended the relevant language of § 512(a) to codify the result of *Netcom*"); ALS Scan, Inc. v. RemarQ Cmtys., Inc., 239 F.3d 619, 622

that section 512(a) should be read as a direct codification of the *Netcom* approach. However, a reading implying such a strong endorsement of *Netcom* is misplaced. Other elements of the legislative history make no mention of the case,[54] and the Senate Judiciary Committee report itself backs away from attempting to establish "a wholesale clarification" of ISP liability through section 512(a).[55] Rather, the Senate Judiciary Committee described its attempt as one of enabling the precedent to continue to evolve.[56] As a result, section 512(a) creates a structure that very much resembles the *Netcom* approach of a shield for infringement helped along by the standard, automatic processes of ISPs, while at the same time it stands apart from the case. Indeed, *Netcom* has continued to survive and develop as relevant precedent alongside section 512(a).

III. POLICING COPYRIGHT INFRINGEMENT & MANAGING NETWORKS

In the years since the explosion of copyright infringement online, there have been a variety of efforts by rights holders to slow its growth and regain some ground. For the most part, these efforts have involved tactics by rights holders alone — through litigation, lobbying, or education. Increasingly, however, ISPs have been pulled into the anti-infringement campaign either through legislative mandate or private agreement.[57] Although it is these ISP-centric measures this paper is primarily concerned about, a brief overview of non-ISP anti-infringement efforts provides important background context.

A. Non-ISP Anti-Infringement Efforts

In the wake of Napster and the early post-Napster peer-to-peer clients, the Recording Industry Association of America ("RIAA") and

(4th Cir. 2001) (referring to "Congress' codification of the *Netcom* principles in Title II of the DMCA."). *See also* CoStar Grp., Inc. v. LoopNet, Inc., 373 F.3d 544, 548, 552–53 (4th Cir. 2004) (describing and rejecting the plaintiff's claim that because the DMCA codified *Netcom* it also supplanted it as functional precedent).

53. *See, e.g.*, Hayes, *supra* note 8, at 22 (describing section 512(a) as "essentially a codification of the *Netcom* case and a rejection of [*Frena*]"); David Ludwig, *Shooting the Messenger: ISP Liability for Contributory Copyright Infringement*, B.C. INTELL. PROP. & TECH. F., Nov. 7, 2006, at 5 ("The legislative history indicates that § 512(a) was intended to codify the holding in *Netcom* . . . .").

54. *See, e.g.*, H.R. REP. NO. 105-551 (1998).

55. *See* S. REP. NO. 105-190, at 19 (1998).

56. *See id.* They did not recognize the irony, it seems, of expressing their desire to "leave [the] current law in its evolving state" in one sentence, then in the next announcing the creation of safe harbors that would specifically block the evolution of the law in a particular direction. *Id.*

57. *See infra* Part III.B.

other representatives of the record industry engaged in a range of education campaigns. These ranged from large-scale, print-based advertisements featuring celebrities like Elton John and Britney Spears to targeted websites informing visitors about copyright law.[58] One such effort involved directly contacting users of KaZaA and Grokster through those programs' chat functions to head them off with warnings about the illegality of their actions.[59] These efforts have continued,[60] though at times they have been subject to the criticism that they only serve to spread misinformation about copyright.[61]

The record industry has also pursued litigation against those making prominent file sharing programs, including Napster, Grokster, KaZaA, Bearshare, and LimeWire — with many reaching settlements mandating their permanent shut-down.[62] By the record industry's own account, this strategy has been a success: the *2012 IFPI Digital Music Report* attributes a drop of seven percentage points in the rate of U.S. file-sharers between 2007 and 2010 to this type of litigation.[63] It is important to note that early on in this series of cases, it was not clear whether peer-to-peer networks would have qualified for the section 512(a) safe harbor. In an unreported opinion, Judge Patel denied summary judgment to Napster on the grounds that it did not qualify for the safe harbor, reasoning that Napster did not itself "transmit, route, or provide connections through its system" but rather those

58. *See, e.g.*, Jennifer Norman, Note, *Staying Alive: Can the Recording Industry Survive Peer-to-Peer?*, 26 COLUM. J.L. & ARTS 371, 403–04 (2003) (describing a print-based campaign involving those celebrities and a number of other efforts to educate consumers on the issue of online infringement); Wendy M. Pollack, Note, *Tuning in: The Future of Copyright Protection for Online Music in the Digital Millennium*, 68 FORDHAM L. REV. 2445, 2470 (2000) (describing the RIAA educational website, soundbyting.com).

59. John Borland, *RIAA to File Swappers: Let's Chat*, CNET NEWS (Apr. 29, 2003, 3:40 PM), http://news.cnet.com/2100-1025_3-998825.html.

60. *See, e.g.*, CAMPUS DOWNLOADING, http://www.campusdownloading.com (last visited Dec.20, 2013). The RIAA acknowledges its association with this website in its FAQ. *See For Students Doing Reports*, RIAA, http://www.riaa.com/faq.php (last visited Dec. 20, 2013).

61. *See, e.g.*, Mike Masnick, *Totally False Propoganda About File Sharing Being Given to Students as Educational Material*, TECHDIRT, (Aug. 22, 2008, 12:08 PM), http://www.techdirt.com/articles/20080822/0233162059.shtml.

62. *See* Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913 (2005); A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001); Arista Records LLC v. Lime Group LLC, 784 F. Supp. 2d 398 (S.D.N.Y. 2011); Eric Pfanner, *Record and Movie Industries Reach a Settlement with Kazaa*, N.Y. TIMES, July 28, 2006, at C3, *available at* http://www.nytimes.com/2006/07/28/technology/28kazaa.html; Ed Oswald, *BearShare Settles with RIAA for $30m*, BETANEWS (May 5, 2006), http://betanews.com/2006/05/05/bearshare-settles-with-riaa-for-30m/.

63. *See* IFPI, *Digital Music Report 2012* at 21 http://www.ifpi.org/content/library/DMR2012.pdf.

connections are made through the Internet (and, presumably, the relevant ISPs).[64]

A third prominent way in which rights holders have sought to alter the course of infringement online has been to sue individual file-sharers directly.[65] The record industry pursued these lawsuits from 2003 through 2008, targeting an estimated 18,000 people, and creating a considerable uptick in copyright litigation in the U.S.[66] Two well-known examples are the sagas of Jammie Thomas-Rasset in Minnesota and Joel Tenenbaum in Massachusetts, who were among the few that mounted a defense rather than settle.[67]

B. ISP-Centric Anti-Infringement Efforts

Despite the progress achieved by these parallel strategies, online copyright infringement continues to thrive and rights holders remain eager to find more effective methods — increasingly those methods involving ISPs.[68] This section provides a background on some of these methods, both those that have been or are currently in effect as well as those which remain merely possible or speculative.

1. Graduated Response

Graduated response has been a favored option for rights holders both nationally and internationally.[69] "Graduated response" generally refers to the cooperation between ISPs and rights holders to identify and punish infringers without having to rely on traditional legal ave-

---

64. *See* A & M Records, Inc. v. Napster, Inc., No. C 99–05183 MHP, 2000 WL 573136, at *8 (N.D. Cal. May 12, 2000).

65. *Recording Industry Begins Suing P2P File Sharers Who Illegally Offer Copyrighted Music Online*, RIAA (Sep. 8, 2003), http://www.riaa.org/newsitem.php?id=85183A9C-28F4-19CE-BDE6-F48E206CE8A1.

66. *See* David Kravets, *Copyright Lawsuits Plummet in Aftermath of RIAA Campaign*, WIRED.COM (May 18, 2010, 1:24 PM), http://www.wired.com/threatlevel/2010/05/riaa-bump.

67. *See, e.g.*, Nate Anderson, *File-Sharer Will Take RIAA Case to Supreme Court*, ARS TECHNICA (Sep. 11, 2012, 6:00 PM), http://arstechnica.com/tech-policy/2012/09/file-sharer-will-take-riaa-case-to-supreme-court; Elinor Mills, *Court Affirms $675,000 Penalty in Music-Downloading Case*, CNET NEWS (Aug. 23, 2012, 4:04 PM), http://news.cnet.com/8301-13578_3-57499519-38/court-affirms-$675000-penalty-in-music-downloading-case; *RIAA Should Pay for Single Mom's Two-Year Ordeal*, Electronic Fronteir Foundation (July 6, 2007), https://www.eff.org/deeplinks/2007/07/riaa-should-pay-single-moms-two-year-ordeal ("few . . . have fought back, resisting RIAA pressure to pay settlement monies").

68. *See, e.g.*, IFPI, *supra* note 63 (expressing optimism about new efforts to reduce infringement through cooperation with ISPs).

69. *See* Annemarie Bridy, *ACTA and the Specter of Graduated Response*, 26 AM. U. INT'L L. REV. 559, 559–60 (2011) (describing the international lobbying efforts for graduated response as well as noting its national-level implementations in the U.K., France, South Korea, and Taiwan).

nues.[70] The most commonly noted model combines independent investigation by rights holders with escalating notices from ISPs to users concerning their alleged infringement and culminates with blocking or hobbling that user's Internet access.[71]

France was one of the first countries to legislatively implement such a system, referred to as HADOPI.[72] HADOPI follows the core model of private detection, notice, and service disruption, but layers a degree of judicial oversight at the penalty phase.[73] Since its implementation in 2010 during the Sarkozy administration, HADOPI has encountered a colder reception by the administration of Francois Hollande, such that the law will likely see drastic changes.[74] This comes despite reports from the agency that its efforts have reduced infringement via peer-to-peer systems.[75]

The United States has started the process of taking a different approach to graduated response, relying not on legislative mandate, but rather on private agreements between rights holders and ISPs, often referred to as "six strikes" for its planned six tiers of notification.[76] The six strikes system will be overseen by the Center for Copyright Information, a group formed by the major rights holder organizations (RIAA, Motion Picture Association of America) and the major ISPs (AT&T, Comcast, Cablevision, Time Warner Cable, Verizon) along with an advisory board of consumer and privacy advocates.[77] Many of

---

70. *See Private Ordering*, *supra* note 11, at 83–84. Bridy's definition of graduated response encompasses a bit more than mine does. While she includes filtering efforts as a form of graduated response, I will deal with that topic separately as it implicates a change in the nature of ISP activity that could be legally relevant to the standard proposed here.

71. *Id.*

72. HADOPI is an acronym for the agency created to oversee the graduated response mechanism: *Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet*. *See* HADOPI, http://www.hadopi.fr/ (last visited Dec. 20, 2013).

73. *See* Nathan Lovejoy, Note, *Procedural Concerns with the HADOPI Graduated Response Model*, HARV. J.L. & TECH. DIG., Jan. 13, 2011, http://jolt.law.harvard.edu/digest/copyright/procedural-concerns-with-the-hadopi-graduated-response-model/ (listing each step of the HADOPI procedure).

74. *See, e.g.*, Cyrus Farivar, *French Anti-P2P Agency Hadopi Likely to Get Shut Down*, ARS TECHNICA, (Aug. 3, 2012, 4:40 PM), http://arstechnica.com/tech-policy/2012/08/french-anti-p2p-agency-hadopi-likely-to-get-shut-down/; Manon Rescan, *Les Allers-Retours de Francois Hollande sur Hadopi* , LE MONDE (May 13, 2013, 7:34 PM), http://www.lemonde.fr/politique/article/2013/05/13/les-allers-retours-de-francois-hollande-sur-hadopi_3176411_823448.html.

75. *See* HADOPI, 1 ½ YEAR AFTER THE LAUNCH, http://www.hadopi.fr/sites/default/files/page/pdf/note17_en.pdf, *also available at* http://www.scribd.com/doc/87387866/Hadopi-Report.

76. *See* Cyrus Farivar, *"Six Strikes" Internet Warning System* Will *Come to US this Year*, ARS TECHNICA (Sep. 11, 2012, 12:10 PM), http://arstechnica.com/tech-policy/2012/09/six-strikes-internet-warning-system-really-truly-coming-to-us-this-year/. The "six strikes" term also represents the over-extension of a tired, but seemingly inescapable, baseball metaphor.

77. *About the Center for Copyright Information*, CENTER FOR COPYRIGHT INFORMATION, http://www.copyrightinformation.org/about (last visited Dec. 20, 2013). It is worth noting

the details of the six strikes system have not yet been revealed, as it has not yet launched. It is important to note that it is colorable that ISPs are required to implement a system along these lines under the repeat infringer policy requirement of section 512(i).[78]

2. Protocol-Specific Traffic Throttling

Another method that could be used as a mechanism to curb online infringement is the throttling of certain types of traffic travelling over ISPs' networks. ISPs have implemented such restrictions in the past for the purpose of network load management and not with an explicit justification of suppressing infringement.[79] The most prominent example of traffic throttling was in 2007 when it was revealed that Comcast had been restricting traffic that employed the BitTorrent protocol — a peer-to-peer protocol used by many file sharing applications.[80] This episode ultimately led to the restriction of the Federal Communication Commission's ("FCC") ability to regulate network management practices.[81] As a result, throttling, or network management techniques more generally, could play a role in attempts to hamper copyright infringement in the future.

3. Higher Education Opportunity Act

Not all of the ISP-centric efforts in the United States have been conducted at the industry level. The Higher Education Opportunity Act ("HEOA") of 2008 conditions federal funds for student aid programs on colleges and universities, in their capacity as ISPs for their campuses, "develop[ing] plans to effectively combat the unauthorized distribution of copyrighted material, including through the use of a variety of technology-based deterrents . . . ."[82] This goes a step further than the vague requirement of section 512(i) to implement a repeat infringer policy by mandating "technology-based deterrents" and stip-

---

that the advisory board includes the President of the notably copyright-skeptical group, Public Knowledge. *See* Gigi Sohn, *Why I Joined the Copyright Alert System Advisory Board*, PUBLIC KNOWLEDGE (Apr. 3, 2012), http://publicknowledge.org/blog/why-i-joined-copyright-alert-system-advisory-.

78. *See supra* notes 35–37 and accompanying text.

79. *See Network Management Update*, COMCAST, http://xfinity.comcast.net/terms/network/update/ (last visited Dec. 20, 2013) (describing network management techniques following the FCC's ruling in *Free Press & Pub. Knowledge Against Comcast Corp*. 23 FCC Rcd. 13028, 13028 (2008)).

80. For an overview of Comcast's throttling during this period, see Andrew Gioia, Note, *FCC Jurisdiction over ISPs in Protocol-Specific Bandwidth Throttling*, 15 MICH. TELECOMM. & TECH. L. REV. 517, 520–22 (2009).

81. *See* Comcast Corp. v. F.C.C., 600 F.3d 642 (D.C. Cir. 2010).

82. 20 U.S.C. § 1094(a)(29)(A) (2012).

ulating that the plans be "effective[]."[83] Though no specific measures are mentioned in the statute, the legislative history points to techniques that go beyond what most commercial ISPs have been engaged in to date.[84]

Colleges and universities represent an edge-case when it comes to ISPs. Given their limited scale, university networks are sometimes designed such that all outgoing traffic travels through a limited number of points.[85] This makes the implementation of "effective deterrents" easier than it would be for commercial ISPs whose traffic patpatterns do not reliably reach such choke points. Regardless, HEOA demonstrates the willingness of Congress to legislate in this arena.

4. Content-Sensitive Deep Packet Inspection

The protocol-specific throttling mentioned above employs a technique called "deep packet inspection" ("DPI") to distinguish one type of traffic from another.[86] DPI uses specialized equipment to identify the contents of discrete units of information (packets) as they travel through ISPs' networks.[87] In the Comcast/BitTorrent scenario, Comcast was using the technology to find out over which protocol the information was travelling but not (as far as we know) to view or record the substantive information.[88]

The ability to determine network operation based on the substantive content of Internet traffic is more than mere theory; rather, it is a capability that equipment manufacturers actively seek to achieve.[89] It is not hard to imagine a very effective copyright infringement policing system on the commercial ISP level that employs content-sensitive DPI to look for particular identifying information attached to copyright protected works and route, record, or block that information ac-

83. *Id.*

84. *See* Annemarie Bridy, *Why Pirates (Still) Won't Behave: Regulating P2P in the Decade After Napster*, 40 RUTGERS L.J. 565, 597 (2009) (discussing the technological methods mentioned in the legislative history of the Higher Education Opportunity Act).

85. *See, e.g.*, LARRY L. PETERSON &BRUCE S. DAVIE, COMPUTER NETWORKS: A SYSTEMS APPROACH, 202, 749 (Rick Adams & Nate McFadden eds., 2012).

86. Free Press & Pub. Knowledge Against Comcast Corp., 23 FCC Rcd. 13028, 13050–51 (2008) ("Comcast has deployed equipment across its networks that monitors its customers' TCP connections using deep packet inspection to determine how many connections are peer-to-peer uploads.").

87. *See* Kevin Werbach, *Breaking the Ice: Rethinking Telecommunications Law for the Digital Age*, 4 J. TELECOMM. & HIGH TECH. L. 59, 92 (2005).

88. *See supra* notes 79–80 and accompanying text.

89. 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, 653 (2008).

cordingly. In fact, commercial products already offer such services to colleges and universities seeking to comply with the HEOA.[90]

IV. STANDARDS FOR FALLING OUT OF SECTION 512(A)

Within the range of potential ISP-centric anti-infringement measures, the question arises: which ones, if any, sufficiently affect ISPs' operations so as to prevent them from claiming the section 512(a) safe harbor? Additionally, what sort of anti-infringement measures *can* ISPs take in the future without running that risk? Of those measures discussed in Part III, the "six strikes" style of graduated response appears to be a relatively safe move given its colorable grounding in section 512(i), and it remains a useful example against which to test the scope of potential standards. Protocol- and content-specific DPI move the ISP further away from the model of dumb intermediary that seems to be sketched out by the provisions of sections 512(a) and (k) as well as the legislative history, but they do not have an equivalent plausible statutory imprimatur. Yet there is very little guidance as to how a court should measure how much interference is permitted before an ISP — the core target of the section 512(a) safe harbor protection — falls out of that zone of safety.

This Part proposes three such potential standards for falling out of section 512(a). The first, a strict neutrality standard, would read the language of sections 512(a) and (k) to require ISPs to do nothing to discriminate between types of traffic that flow over their networks in order to retain the safe harbor protection. The second, a knowledge-based approach, would read sections 512(a) and (k) in the context of the parallel *Netcom* standard to permit some types of manipulations but not others. The third would read section 512(a) at a high level of generality to condition protection on ISPs' actions falling within the category of conduit, rather than editorial. In discussing each standard, this paper will first outline its operation and then address its advantages and flaws.

A. Option 1: Neutrality Standard

A number of commentators have suggested that operation of a non-neutral network would be enough to push ISPs out of section 512(a) protection.[91] This perspective is based on the idea that as soon

90. *See* Alexandre M. Mateus & Jon M. Peha, *P2P on Campus: Who, What, and How Much*, 7 I/S: J. L. & POL'Y FOR INFO. SOC'Y 257, 262–63 (2012) (describing commercial filtering options Copysense and Packeteer that employ DPI). *See also Private Ordering*, *supra* note 11, at 84.

91. *See, e.g.,* Frieden, *supra* note 89, at 656–59 (arguing that ISP packet discrimination and qualification for DMCA safe harbors are inconsistent); Alex Pisarevsky, Note, *COPE-*

as an ISP begins treating certain bits of information differently from others, it is no longer engaged in network operation that could fall under the heading of transferring information between third parties via an "automatic process" as required by section 512(a).[92] Such an approach would permit six strike graduated response mechanisms — though it would perhaps block those that degraded the connections of alleged infringers to the extent the ISP would be treating that category information in a disfavored fashion. DPI, on both content- and protocol-sensitive grounds, would be grounds for loss of safe harbor protection as it constitutes an affirmative step away from the automatic, neutral routing of information over the network.

There are two main advantages to employing the neutrality standard for drawing the outer bounds of section 512(a) protection. First, it comes closer to rule-like clarity than the standards discussed below. It sets a relatively clear line across which ISPs may not pass if they want to retain the safe harbor — namely, if ISPs meddle with the operation of their network to make it something other than a *dumb* conduit for communication, they would open themselves to liability for infringement over their networks. Regardless of whether ISPs would find this just, they would at least be able to act accordingly to protect themselves.

Second, to the extent that one subscribes to the benefits of neutral networks — including the prevention of centralized control or the encouragement of content-level innovation[93] — reading a statutory requirement for those principles into sections 512(a) and (k) is very convenient. Rather than having to rely on the D.C. Circuit's interpretation of FCC authority[94] or wait for Congress to legislate directly on the issue, network neutrality advocates can simply point to section 512(a) as preexisting codification of the matter. Naturally, this benefit extends only as far as one's definition and support of network neutrality and its benefits. This approach also meshes well with the implica-

---

Ing with the Future: An Examination of the Potential Copyright Liability of Non-Neutral Networks for Infringing Internet Content, 24 CARDOZO ARTS & ENT. L.J. 1359, 1383 (2007) ("For a network operator, abandoning the principles of net neutrality to construct a tiered network could potentially amount to a waiver of OCILLA's protections from copyright liability.").

92. *See* Pisarevsky, *supra* note 91, at 1383.

93. For examples of the positive case for network neutrality, there are few better sources than the work of Tim Wu. *See, e.g.,* Tim Wu, *Network Neutrality, Broadband Discrimination*, 2 J. ON TELECOMM. & HIGH TECH. L. 141 (2003); Tim Wu, *Why You Should Care About Network Neutrality*, SLATE (May 1, 2006, 4:35 PM), http://www.slate.com/articles/technology/technology/2006/05/why_you_should_care_about_network_neutrality.html.

94. The D.C. Circuit heard oral arguments in *Verizon v. FCC* in September 2013. Verizon has challenged the FCC's open Internet rules. Edward Wyatt, *Verizon-F.C.C. Court Fight Takes on Regulating Net*, N.Y. TIMES, Sept. 9, 2013, at B1, available at http://www.nytimes.com/2013/09/09/business/verizon-and-fcc-net-neutrality-battle-set-in-district-court.html?_r=1&.

tion made by the *Netcom* court that if Netcom had "completely relinquish[ed] control over how its system [was] used" it would have been in a better position to avoid secondary liability.[95]

The neutrality standard runs into trouble in a number of areas. First, there is a definitional problem — it is difficult to nail down what exactly constitutes network neutrality and what its goals should be.[96] Certainly, one can imagine a spectrum of interpretations of what should constitute an "automatic process" for the purposes of identifying non-neutrality. At what point in the scope of packet discrimination does it become "automatic"? As a result, yoking section 512(a) protection to network neutrality simply pushes the determination for loss of protection off to a hotly contested policy fight over the meaning of "neutrality." Rather than producing clarity for ISPs and courts, this standard could add another layer of confusion.

Furthermore, the concept of network neutrality exists in a politically and legally uncertain state. ISPs have aggressively lobbied against the imposition of network neutrality rules,[97] while Internet activists and major web content providers have just as vigorously championed them.[98] On the legal front, the D.C. Circuit has curbed the FCC's ability to mandate network neutrality rules as a result of the Commission's attempt to restrict Comcast's BitTorrent throttling attempts.[99] To tie section 512(a) applicability so closely to a political third-rail would not help in crafting sensible policy decisions that could reliably be employed by courts.

A second flaw is that employing a neutrality standard could materially impact non-copyright related actions that have little connection to copyright-related liability. For instance, if an ISP were engaging in packet discrimination to implement a tiered-access system,[100] it would lose its safe harbor for copyright liability. The merits of prohibiting

---

95. *See* Religious Tech. Ctr. v. Netcom On-Line Commc'n Services, Inc., 907 F. Supp. 1361, 1375 (N.D. Cal. 1995).

96. *See* Jon M. Peha, *The Benefits and Risks of Mandating Network Neutrality, and the Quest for a Balanced Policy*, 1 INT'L J. COMM. 644, 657–64 (2007), http://ijoc.org/ojs/index.php/ijoc/article/viewFile/154/90 (surveying a variety of definitions of "network neutrality" and proposing his own).

97. *See, e.g.*, Alex Chasick, *AT&T Asks Employees to Oppose Net Neutrality,* CONSUMERIST (Oct. 20, 2009), http://consumerist.com/2009/10/20/att-asks-employees-to-oppose-net-neutrality/.

98. *See, e.g.,* Joel Rothstein, *Google Founder Lobbies for Net Neutrality*, COMPUTERWORLD (Jun. 7, 2006, 12:00 PM), http://www.computerworld.com/s/article/9001000/Google_founder_lobbies_for_Net_neutrality; Tony Bradley, *Parties Lobby FCC on Net Neutrality*, PCWORLD (Jan. 15, 2010, 9:37 AM), http://www.pcworld.com/article/187003/Parties_Lobby_FCC_on_Net_Neutrality.html.

99. Comcast Corp. v. F.C.C., 600 F.3d 642 (D.C. Cir. 2010). *See also supra* notes 79–81 and accompanying text.

100. A system under which some online services are able to pay ISPs for improved connections to their subscribers.

tiered services aside, it would seem strange to condition the rights and protections of an ISP in the copyright realm on its actions in areas that have nothing to do with its facilitation or knowledge of copyright infringement.

B. Option 2: Knowledge-Based Standard

A second option for delineating the scope of section 512(a) is to draw aspects from the *secondary* infringement standards detailed in the *Netcom* line of cases. After all, it was *Netcom*'s analysis of direct infringement that may have inspired the safe harbor originally.[101] Indeed, one early draft of the DMCA in part qualified section 512(a) protection on the secondary liability standards for knowledge,[102] which was also the primary subject of contention in *Netcom*'s discussion of secondary liability.[103] If secondary infringement standards were used to interpret the bounds of the section 512(a) requirements, the degree to which measures taken by ISPs tend to result in the actual or constructive knowledge of infringing activities should be a critical factor in determining whether those activities are sufficient to push the ISP out of the safe harbor.

For instance, if an ISP were to implement a mechanism that tracked or manipulated the volume of traffic on the basis of content-type, on a user-by-user basis, this would bolster the case for its constructive knowledge of infringing activities regardless of whether or not the mechanism was intended to police infringement. Such actions would thus push liability for activities subject to this mechanism out of section 512(a) protection. On the other hand, if the ISP were to implement a system of tiered access based only on the identity of the subscriber, it would be unrelated to the elements of constructive knowledge.

Under this knowledge-based standard, the six strikes approach to graduated response would clearly be safe, as it relies on notification from rights holders about alleged infringement — exactly the sort of action the *Netcom* court rejected as sufficient knowledge.[104] "Network management"-targeted DPI, in the form of Comcast's BitTorrent throttling, would also plausibly not be sufficient to strip section 512(a) protection, as knowledge of protocol-level information would not likely lead to constructive knowledge of infringement. However, content-sensitive DPI and filtering would probably be a step too far under

101. *See supra* notes 39–56 and accompanying text.

102. *See* 6 Patry on Copyright § 21:85 (2013).

103. *See* Religious Tech. Ctr. v. Netcom On-Line Commc'n Services, Inc., 907 F. Supp. 1361, 1373–75 (N.D. Cal. 1995).

104. *See id.* at 1373–74.

a knowledge-based standard. There, ISPs would have specific information about the volumes of specific copyright protected content that could easily lead to constructive knowledge in the right context.

The knowledge-based approach is doctrinally attractive as it would acknowledge the role of *Netcom* in influencing DMCA safe harbors by using that standard to add interpretive color.[105] Additionally, a knowledge-based standard would permit greater flexibility, allowing ISPs to implement efficiency-creating network technologies, that, under a neutral network standard, might expose them to copyright liability. Furthermore, there is a structural appeal in limiting section 512(a) to actions by ISPs that materially affect their relationship to copyright infringement and to leave all other actions out of the realm of regulatory copyright.[106]

Despite some flexibility and doctrinal neatness that a knowledge-based standard might generate, it does not come without substantial problems. First, and perhaps most obviously, grounding part of the justification on the inclusion of a knowledge standard in an early draft of the legislation is problematic. Surely, if Congress intended for courts to apply a knowledge-based standard for actions that push outside of section 512(a), it would not have removed it from the final draft. In response, one could read its exclusion as an attempt to leave a knowledge-based standard open for courts to apply without limiting the development of the standard. Either way, the fleeting reference in the legislative history raises more questions than it answers.

Second, tying section 512(a) eligibility too closely to *Netcom* and its progeny could have unintended effects. For example, in a 2009 case from S.D.N.Y. — *Arista v. Usenet.com* — the court found that filtering and management of non-copyright related subject matter indicated sufficient volition on the part of the service provider to create direct liability.[107] As Annemarie Bridy has pointed out, if this same standard were imported to section 512(a) eligibility (presumably on the argument that *Netcom*'s direct infringement analysis inspired its creation) ISPs would face even greater restrictions on their ability to act than under the neutral network standard.[108]

Third, a knowledge-based standard could merely encourage acts of willful blindness on the part of ISPs eager not to lose section 512(a) protection and reveal the blurry definitional lines at work under the surface. Where this could occur in the examples provided in this paper is in the distinction between protocol- and content-sensitive DPI. Be-

105. *See supra notes* 39–56 and accompanying text.

106. For a discussion of copyright as a means of communications policy, see Timothy Wu, *Copyright's Communications Policy*, 103 MICH. L. REV. 278 (2004).

107. *See* Arista Records v. Usenet.com, 633 F. Supp. 2d 124, 148–49 (S.D.N.Y. 2009).

108. *See Private Ordering*, *supra* note 11, at 120–24 (discussing that case's potential implications for the implementation of "smart network technolog[ies]").

cause the mechanism at work in either case is not technologically different, ISPs are able to choose the level of information to which they are exposed.[109] Gathering content-level information when one is already gathering protocol information is a matter of decision-making and operational resources only, not a hard technological limit. As a result, ISPs would be incentivized to consciously avoid certain types of information that they might otherwise easily come upon, and courts would have to wade into the fine lines between DPI aimed at network management and DPI aimed at content detection.

C. Option 3: Conduit Versus Editorial Mechanisms Standard

A third approach to determining the limits of section 512(a) eligibility would be categorical: a court would determine whether, in light of any particular mechanism or combination of mechanisms, an ISP is functioning as a conduit or as an editor. To justify this approach, one would have to read the text and history of section 512(a) at a relatively high level of generality, noting that the requirements for inclusion tend to describe conduit functions in contrast to the more editorial-like functions that are protected under other safe harbors or not at all. Indeed, there is some support in the legislative history for such an interpretation of the intent of the drafters.[110] Applying the conduit/editorial approach to the mechanisms discussed in this paper, the results would be similar to those under the knowledge-based standard: six strikes graduated response would introduce few editorial-like functions, but content-sensitive DPI might characterize an ISP as acting in an editorial capacity, thus endangering their section 512(a) protection.

The advantage of the conduit/editorial standard is that it leaves the door open for technological progress in a way that the neutral network standard might make more difficult — for instance, by permitting the implementation of network management techniques (regardless of the technology used to achieve them) that simply allow the ISP to perform its conduit-related functions more efficiently or profitably. Unlike the knowledge-based standard, it does not risk tying that flexibility to the development of a parallel set of case law. It also has the appeal of building some suppleness and technology-neutrality into the hard-edged environment of the DMCA. This could stretch that statutory scheme's useful life a bit longer against the changing face of ISP technical limits.[111]

---

109. *See* ELEC. PRIVACY INFO. CTR., A NATIONAL BROADBAND PLAN FOR OUR FUTURE, COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER at 7 (2009), *available at* http://epic.org/privacy/pdf/fcc_broadband_6-8-09.pdf.

110. *See supra* note 30 and accompanying text.

111. *See Private Ordering*, *supra* note 11, at 123–24 (noting the changing technological environment).

The problems with the conduit/editorial standard combine those of the neutrality and knowledge-based standards. First, like the neutral network standard, this approach would tend to expose ISPs to copyright liability for actions that are not materially related to the flow of copyright infringement, so long as they tended to be editorial in nature. Second, even more than the knowledge-based standard, this approach has flimsy structural or textual justification, relying on impli-implication and legislative history alone. While it may be appealing from a holistic sense, it would require interpretation at a level of generality to which the text of the DMCA does not seem accommodating.

D. Caveat: Expansion of Safe Harbor Through Section 512(i) Standard Technical Measures

The important role of the section 512(i) standard technical measures requirement bears mentioning in the discussion of designing standards to gauge whether ISP-implemented mechanisms affect section 512(a) eligibility. Under any of these interpretive approaches discussed above, ISPs would still be required to "accommodate[]" copyright policing-related mechanisms that reach such a level of acceptance as to be deemed "standard."[112] To reach this level a "technical [measure] . . . [must] have been developed pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process . . . ."[113] This would be no easy feat (though perhaps the process by which the six strikes system was developed would fit the definition if it were required to)[114] but should it be achieved, it would require ISPs to "accommodate[]" an anti-infringement mechanism regardless of whether it would cause the network to be non-neutral, affect the knowledge of the ISP, or tend to characterize its actions as editorial.

V. CONCLUSION

As ISPs become increasingly able and willing to police copyright infringement that occurs over their networks, they should be wary of actions that might push them out of the section 512(a) safe harbor. This paper has outlined three potential approaches to determining the limits of section 512(a) eligibility for the entities to which that protection is naturally thought to apply. Fortunately for rights holders, the most prominent anti-infringement effort by U.S.-based ISPs so far — the six strikes graduated response system — likely falls within the

112. 17 U.S.C. § 512(i)(1)(B)–(i)(2)(C) (2012).
113. *Id.*
114. *See supra* note 77 and accompanying text.

bounds of all three standards, limiting the risk of this particular activity. Where copyright enforcement may lead to exposure to copyright liability lies with the potential for increased usage of DPI.

Any of the three standards could provide useful clarification for the core group of ISPs that face the possibility of falling out of section 512(a) through their escalating involvement in the transmission of information over their networks. However, none of these standards is entirely satisfying theoretically, doctrinally, or practically. If ISPs continue to feel a growing pressure to develop new and more sophisticated anti-infringement mechanisms, they will one day run up against the limits of section 512(a) protection. In outlining three plausible standards, this paper has pointed to the relative merits and pitfalls that await their implementation.